



INSTALLATION AND UPGRADE GUIDE

Security Event Manager

Version 2024.2.1

© 2024 SolarWinds Worldwide, LLC. All rights reserved.

This document may not be reproduced by any means nor modified, decompiled, disassembled, published or distributed, in whole or in part, or translated to any electronic medium or other means without the prior written consent of SolarWinds. All right, title, and interest in and to the software, services, and documentation are and shall remain the exclusive property of SolarWinds, its affiliates, and/or its respective licensors.

SOLARWINDS DISCLAIMS ALL WARRANTIES, CONDITIONS, OR OTHER TERMS, EXPRESS OR IMPLIED, STATUTORY OR OTHERWISE, ON THE DOCUMENTATION, INCLUDING WITHOUT LIMITATION NONINFRINGEMENT, ACCURACY, COMPLETENESS, OR USEFULNESS OF ANY INFORMATION CONTAINED HEREIN. IN NO EVENT SHALL SOLARWINDS, ITS SUPPLIERS, NOR ITS LICENSORS BE LIABLE FOR ANY DAMAGES, WHETHER ARISING IN TORT, CONTRACT OR ANY OTHER LEGAL THEORY, EVEN IF SOLARWINDS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

The SolarWinds, SolarWinds & Design, Orion, and THWACK trademarks are the exclusive property of SolarWinds Worldwide, LLC or its affiliates, are registered with the U.S. Patent and Trademark Office, and may be registered or pending registration in other countries. All other SolarWinds trademarks, service marks, and logos may be common law marks or are registered or pending registration. All other trademarks mentioned herein are used for identification purposes only and are trademarks of (and may be registered trademarks) of their respective companies.

Table of Contents

SEM deployment examples	5
Simple deployment	5
Complex deployment	6
Prepare to install SEM	7
Plan for the installation	7
Prepare the environment	9
Install and deploy SEM	10
Install SEM on Microsoft Hyper-V	10
Install SEM on VMware vSphere	13
Deploy SEM on Microsoft Azure	15
Deploy SEM using Azure CLI 2.0	16
Deploy SEM on Amazon Web Services	36
Complete the installation	45
Run the setup wizard	45
Activate the SEM license	49
Secure SEM from unauthorized users	52
Install the SEM Agent	56
SEM Agent deployment options	56
SEM Agent pre-installation checklist	57
Install the SEM Agent on Linux and Unix	59
Download the SEM Agent for Windows	61
Run the SEM Remote Agent installer	64
Run the SEM Local Agent installer	67
Verify the SEM Agent connection	69
Upgrade SEM	71
Determine the SEM upgrade path	71
Best practices for SEM upgrades	81
Upgrade the SEM components	82
Upgrade the virtual appliance	82

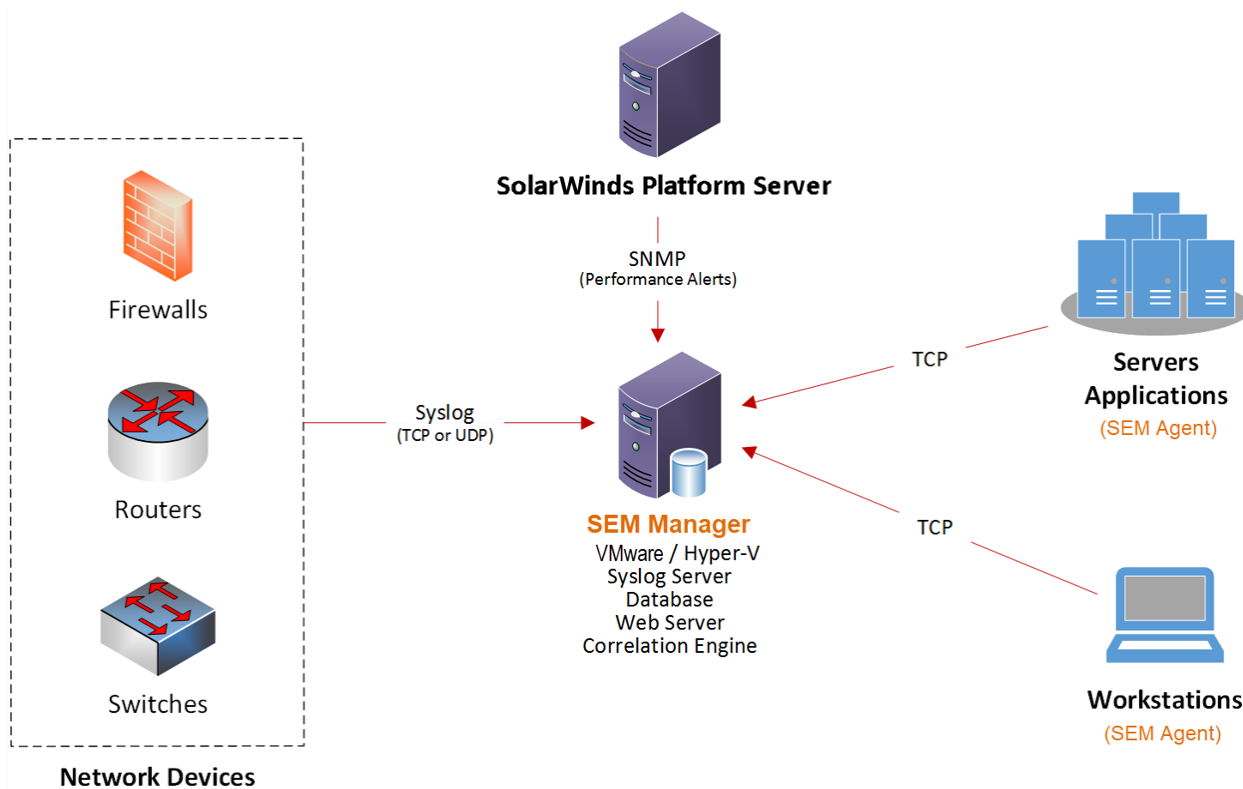
Mount the ISO image file	85
Upgrade to SEM 6.4 or later using an ISO	86
Upgrade to SEM 6.4 or later across a network share	90
Upgrade the connectors	91
Upgrade the web console	94
Upgrade the agents	94
Adjust the Agent Updates setting	95
Log in to SEM	97
Log in to the SEM Console	97
Log in to the SEM CMC command line interface	98
Get help after you install SEM	101

SEM deployment examples

This section will help get you started planning your SEM deployment. The examples provide an overview of your SEM deployment options.

Simple deployment

A simple deployment uses one central syslog server to collect log data from your network devices in a local network. In this deployment, network devices use TCP or UDP to send syslog data to the SEM Manager's syslog server, whereas SEM Agents running on workstations and servers just use TCP to push log data to the SEM Manager.

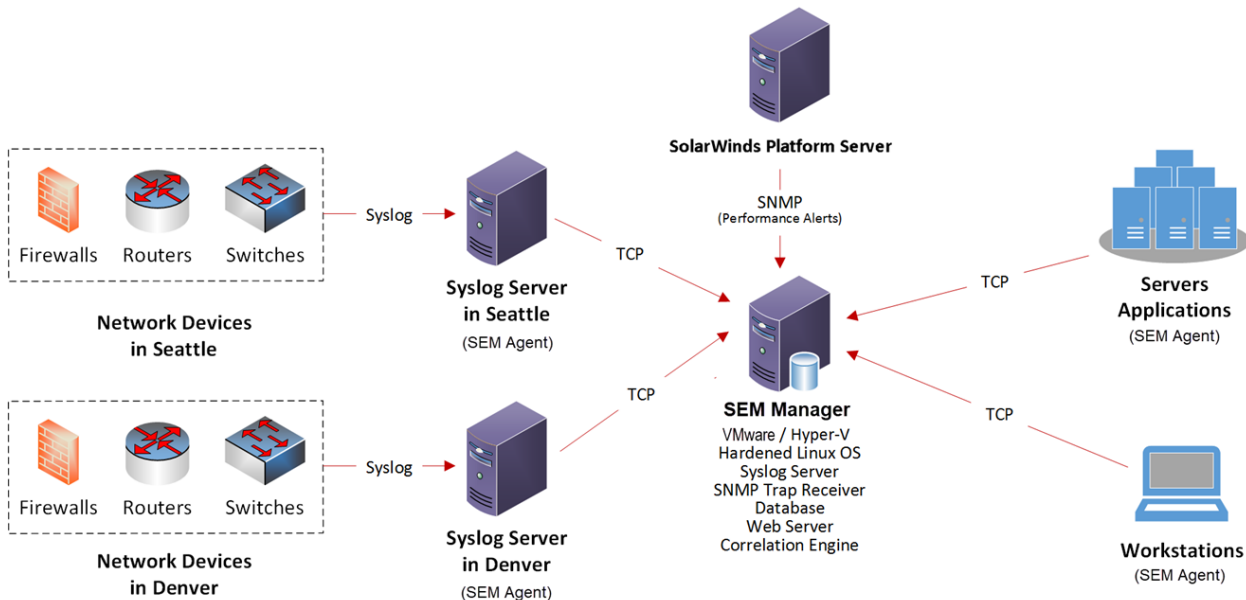


The syslog server receives logs on port 514 and saves the data in the SEM Manager `/var/log` file partition. The log file names vary based on the target facility configured on the network device.

i The SEM Manager relies on routers, firewalls, and switches to transmit syslog messages to the syslog server running on the SEM Manager. For a list of all ports required to communicate with SEM, see the [Port requirements for all SolarWinds products](#).

Complex deployment

A complex deployment uses two syslog servers located in different cities. SEM can capture logs from multiple remote locations across wide area network (WAN) links. Because the SEM agent includes built-in encryption, compression, and buffering capabilities, this deployment can be implemented securely and efficiently.



Instead of using the syslog server built in to SEM Manager, this deployment uses one syslog server for each location. If you implement a detached syslog server, install a SEM agent on each detached server. When you are finished, enable the appropriate connectors on the SEM agent.


After you complete and implement this configuration, the SEM connectors will normalize raw log messages into SEM events.


i If you cannot add new logging hosts on your network devices due to restrictive change management processes, consider implementing this multi-syslog server deployment to leverage your existing syslog servers.

Prepare to install SEM

If you are installing and deploying SEM, complete the pre-installation checklist below. These checklists help you:


- Verify that system requirements are met, all required software is installed, and required roles and features are enabled.
- Gather the information required to complete the installation.

 Be sure to reserve memory and CPU resources for SEM, and not just allocate these resources. See [The reason why SEM needs memory and CPU resource reservations](#) for more information.

 To prevent access by unauthorized users, SolarWinds recommends setting up the SEM appliance with no access to the Internet or any public-facing network. See the [SEM security checklists](#) for additional recommendations.

Plan for the installation

- ☐ Review the Security Event Manager [release notes](#).
- ☐ Identify the environment where SEM will be installed. Ensure that it meets the hardware and software requirements for your installation.
See the [system requirements](#) for details.
- ☐ Create a user profile on the SolarWinds Customer Portal. This profile allows you to download SolarWinds products and licenses.
See [Access the Customer Portal](#) for instructions.
- ☐ Determine if your network architecture will include one or more syslog servers.
See [SEM deployment examples](#) for details.
- ☐ Locate your local administrator account information. This account is required to install SEM.

 The Local Administrator Account is not the same as a domain account with local admin rights. A domain account is subject to your domain group policies.

☐ Create a log in password for your deployment that:

- Does not include the word `username`.
- Includes between 6 and 40 characters.
- Includes at least one uppercase letter.
- Includes at least one lowercase letter.
- Includes at least one digit.

You will need this password when you complete the installation.

☐ Schedule the installation in your environment.

Prepare the environment

Before the installation, prepare the SolarWinds environment:

- ☐ Prepare the servers based on your deployment size and [system requirements](#).
- ☐ Before the installation, **run all operating system updates** on all servers. As you install, if an operating system update runs, your system may reboot and require you to restart the installation process.
- ☐ Open the required ports for your server ports and firewall.


See the SEM port requirements in the [system requirements](#). SEM uses these ports to send and receive data.

Next steps:

- See [Install SEM on Microsoft Hyper-V](#).
- See [Install SEM on VMware vSphere](#).

Install and deploy SEM

You can install SEM on Microsoft Hyper-V, VMware vSphere, Microsoft Azure, and Amazon Web Services. See the following sections for instructions.

 By default, SEM deploys with 8GB RAM and 2 CPUs on both hypervisor platforms.

Install SEM on Microsoft Hyper-V

Access the Customer Portal and download the Security Event Manager Hyper-V Appliance installer. This installer includes a SEM version that you select in the portal.

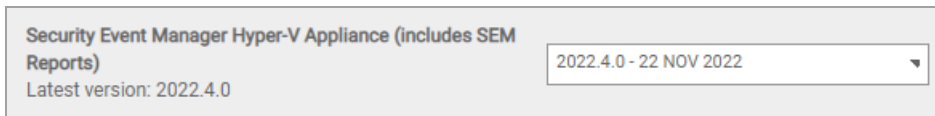
You can also download a free trial version from the [Security Event Manager website](#). The trial version provides unlimited access to all product features for 30 days.

Prepare for the install

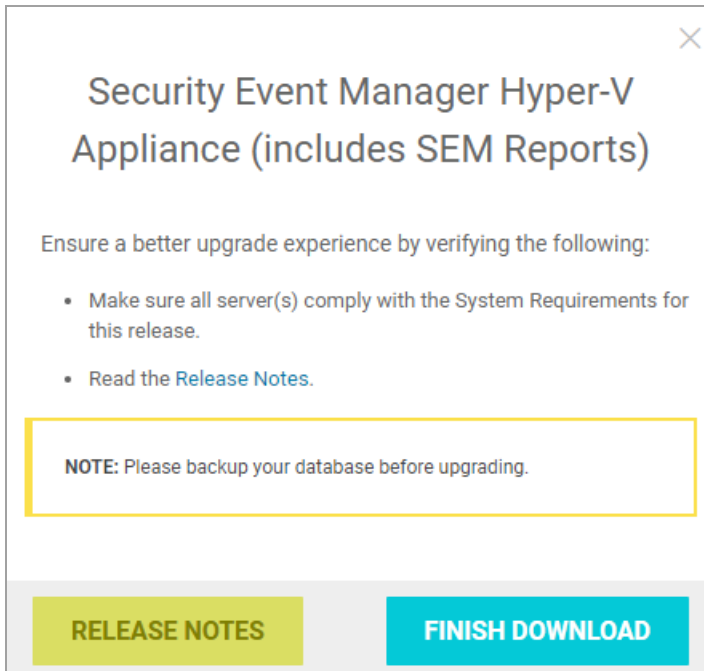
1. Ensure that your Microsoft Hyper-V machine meets all [system requirements](#).
2. Ensure that Volume Shadowcopy is disabled on the Hyper-V machine.
3. Review the [pre-installation checklist](#).

Install SEM

1. Download the installer.
 - a. Quit all other programs.
 - b. Log in to the [Customer Portal](#).
 - c. Click Downloads > Download Product.
 - d. Click the Products drop-down menu and select:
Server Event Manager (SEM), formerly Log & Event Manager (LEM)
 - e. Click the Licenses drop-down menu and select your license tier.
 - f. Under All Release Downloads, locate the Security Event Manager Hyper-V Appliance installer.



- g. Click the product version drop-down menu and select the latest release.
- h. Review the information in the window, and then click Download.



- i. Follow the instructions on your screen to complete the download.

The following executable is downloaded to your desktop folder:

SolarWinds-SEM-<version>-Evaluation-HyperV.exe

where <version> is the product version you selected in the drop-down menu.

2. Extract the files.

In the desktop folder, double-click the EXE file. The extracted files and tools are added to a folder on your desktop.

3. Import the virtual machine.

- a. Open Hyper-V Manager.
- b. In the Hyper-V Manager navigation pane, select the computer running Hyper-V.
- c. Click Action > Import Virtual Machine.
- d. If the Before You Begin screen displays, read the content and then click Next.

- e. On the Locate Folder screen, navigate to the folder that matches your version of Windows Server, and then click Next.

If you are running Windows Server 2016, navigate to the Virtual Machines 2012 R2 folder, and then click Next.

For example:

```
..\SolarWinds-SEM-2022.4-Appliance-HyperV\SolarWinds Security Event  
Manager\Virtual Machines 2012 R2
```

- f. On the Select Virtual Machine screen, select SolarWinds Security Event Manager, and then click Next.
- g. On the Choose Import Type screen, choose Copy the virtual machine (create a new unique ID), and then click Next.
- h. On the Choose Folders for Virtual Machine Files screen, change the folder locations that the wizard will import files to (if needed). Otherwise, click Next.
- i. On the Choose Folders to Store Virtual Hard Disks screen, change the location of the virtual hard disks for this virtual machine (if needed). Otherwise, click Next.
- j. Verify that Volume Shadowcopy is disabled for this virtual Hyper-V machine.
- k. On the Configure Memory screen, configure the Startup RAM setting, and the Minimum RAM and Maximum RAM settings for Dynamic Memory, and then click Next.
- l. On the Summary screen, review the configuration settings and click Finish.

In this example, the installer copies the `SolarWinds-SEM-2022.4.vhd` file to Hyper-V. The file name will vary based on your targeted release version.

4. Connect to the SEM VM.

- a. Select the newly added VM.
- b. In the main Hyper-V Manager window, click Action > Connect.


The virtual console displays on the screen.

5. Start SEM.

- a. In the virtual console window, click Action > Start.

The SEM VM starts.

- b. Record the VM IP Address and keep it in a safe place. You will need this IP address when you [run the setup wizard](#). You can change the IP address later when you configure SEM.

 The default SEM host name is `swi-sem`. To change the default host name and IP address settings, see [Run the activate command to secure SEM and configure network settings](#) in the SEM Administrator Guide for instructions.

6. [Complete the SEM installation.](#)

Install SEM on VMware vSphere

Access the Customer Portal and download the Security Event Manager VMware Appliance installer. This installer includes a SEM version that you select in the portal.

You can also download a free trial version from the [Security Event Manager website](#). The trial version provides unlimited access to all product features for 30 days.

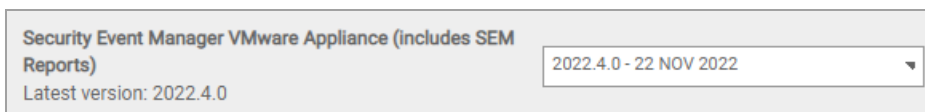
Prepare for the install

1. Ensure that your VMware vSphere machine meets all [system requirements](#).
2. Review the [pre-installation checklist](#).

Install SEM

1. Download the installer.
 - a. Quit all other programs.
 - b. Log in to the [Customer Portal](#).
 - c. Click Downloads > Download Product.
 - d. Click the Products drop-down menu and select:

Server Event Manager (SEM), formerly Log & Event Manager (LEM)
 - e. Click the Licenses drop-down menu and select your license tier.
 - f. Under All Release Downloads, locate the Security Event Manager VMware Appliance installer.



- g. Click the product version drop-down menu and select the latest release.
- h. Click Download.

- i. Follow the instructions on your screen to complete the download.

The extracted files and tools are added to a folder on your desktop.

The How to Install page opens automatically.

2. Extract the files.

In the desktop folder, double-click the EXE file. The extracted files and tools are added to a folder on your desktop. The How to Install page opens automatically.

To return to this page after it is closed, go to:

```
%USERPROFILE%\Desktop\SolarWinds Security Event Manager\html\install_
now.hta
```

3. Deploy SEM.

- a. Start the VMware vSphere client.
- b. Log in with VMware administrator privileges.
- c. Deploy the open virtualization format (OVF) template.
- d. Open the SolarWinds Security Event Manager folder located on your desktop and double-click:

Deploy First—SEM Virtual Appliance.ova

- e. Complete the setup wizard.

When prompted, select the Thin Provisioned disk format.



Thin provisioning offers more performance flexibility than thick provisioning, but requires more oversight than thick provisioning. It also provides increased performance by dedicating physical storage space.

- f. Map the network interface card (NIC) to the appropriate network.
- g. When the OVF deployment is completed, click Finish.

4. Start SEM.

- a. Select the SolarWinds Security Event Manager virtual appliance and click Play.
- b. Click the Console tab.

The SEM VM starts.

- c. Record the VM IP Address and keep it in a safe place. You will need this IP address when you [run the setup wizard](#). You will be able to change the IP address later during the configuration phase.

i The default SEM host name is `swi-sem`. To change the default host name and IP address settings, [run the activate command](#) to secure SEM and configure the network settings.

5. [Complete the SEM installation](#).

Deploy SEM on Microsoft Azure

SEM is not currently available in the Azure Marketplace. However, you can initiate deploying SEM through Azure CLI 2.0.

i The SEM Installation Guide describes the deployment from Windows (PowerShell) and Linux (Bash).

SolarWinds provides a ZIP archive containing two virtual hard disk (VHD) files:

- `xxx-system.vhd` - This file contains an operating system based on Linux Debian.
- `xxx-data.vhd` - This file serves as the data partition. The layout is similar to the VMware and Hyper-V appliances.

Azure CLI 2.0 must be installed on Windows or Linux systems. After the CLI is authenticated, you can control Azure through the API by executing CLI commands.

SEM sizing

For sizing criteria on Microsoft Azure, SolarWinds uses three basic sizes of SEM deployment: small, medium, and large. See the [SEM system requirements](#) for details.

Configure networking

By default, the inbound firewall rule allowing SSH is enabled for a new Linux machine. If required, you can disable SSH from public access for a SEM appliance. To view all default rules created per virtual machine, see [Default security rules](#) located on the Microsoft Learn website for Azure (© Microsoft 2023, available at docs.microsoft.com, retrieved March 20, 2023).

Configure the firewall rules based on your specific needs. The following example shows the security rules for a SEM Azure deployment:

Home > Virtual machines > - Networking > Effective security rules

Effective security rules

Download Refresh

Showing only top 50 security rules in each grid, click Download above to see all.

Select a network interface below to see the effective security rules and network security groups associated with it.

Scope Network interface ()

Associated NSGs: (Network interface)

Click on a rule row to see the expanded list of prefixes.

Inbound rules

NAME	PRIORITY	SOURCE	SOURCE PORTS	DESTINATION	DESTINATION PORTS	PROTOCOL	ACCESS
default-allow-ssh	1000	0.0.0.0/0	0-65535	0.0.0.0/0	22-22	TCP	Allow
AllowVnetInBound	65000	Virtual network (3 prefixes)	0-65535	Virtual network (3 prefixes)	0-65535	All	Allow
AllowAzureLoadBalancer...	65001	Azure load balancer (1 prefixes)	0-65535	0.0.0.0/0	0-65535	All	Allow
DenyAllInBound	65500	0.0.0.0/0	0-65535	0.0.0.0/0	0-65535	All	Deny

Outbound rules

NAME	PRIORITY	SOURCE	SOURCE PORTS	DESTINATION	DESTINATION PORTS	PROTOCOL	ACCESS
AllowVnetOutBound	65000	Virtual network (3 prefixes)	0-65535	Virtual network (3 prefixes)	0-65535	All	Allow
AllowInternetOutBound	65001	0.0.0.0/0	0-65535	Internet (82 prefixes)	0-65535	All	Allow
DenyAllOutBound	65500	0.0.0.0/0	0-65535	0.0.0.0/0	0-65535	All	Deny

Deploy SEM using Azure CLI 2.0

To learn more about installing CLI on Windows and Linux, see [Azure CLI 2.0](#) on the Microsoft website.

To deploy SEM using Azure CLI 2.0, perform the following procedures:

1. [Download and install Azure CLI 2.0 on Microsoft Windows.](#)
2. [Create and manage storage accounts and define resource groups and locations.](#)
3. [Obtain a storage access key.](#)
4. [Prepare to deploy the virtual hard disks.](#)
5. [Enable boot diagnostics.](#)
6. Deploy SEM from [PowerShell \(for Windows\)](#) or [Bash \(for Linux\)](#).

Download and install Azure CLI 2.0 on Microsoft Windows

💡 Learn how to install Azure CLI on Linux or macOS [here](#).

1. Download the Azure CLI 2.0 MSI installer [here](#).

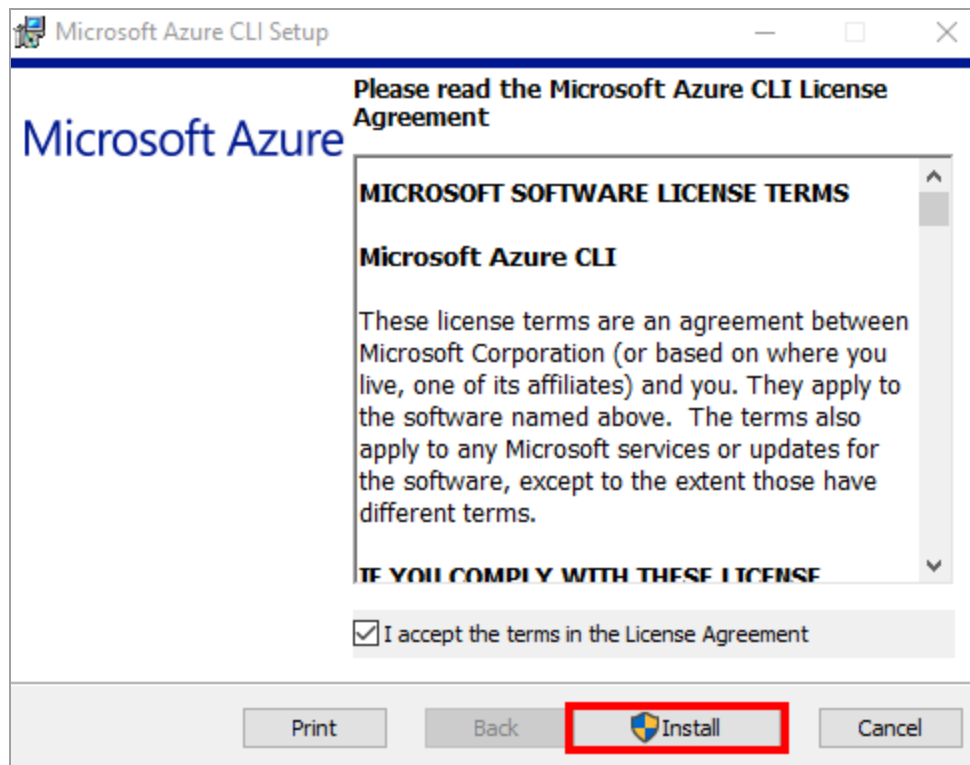
Install or update

The MSI distributable is used for installing or updating the Azure CLI on Windows. You don't need to uninstall any current versions before using the MSI installer.

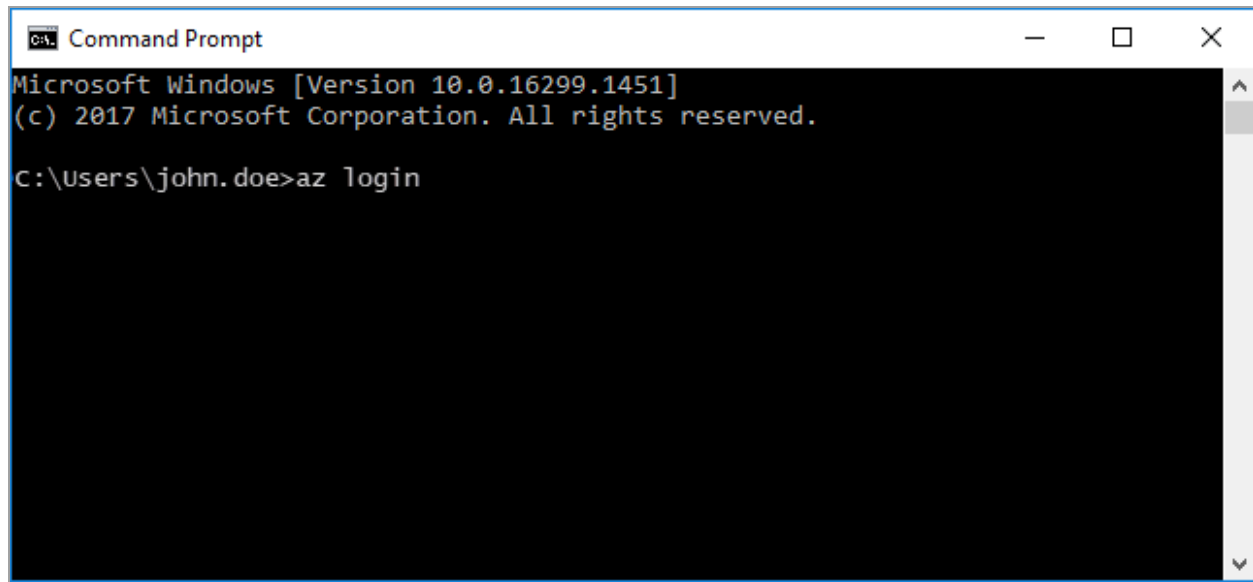
Download the MSI installer

When the installer asks if it can make changes to your computer, click the "Yes" box.


2. Launch the installer, select the check box if you accept the License Agreement terms, and then click Install.



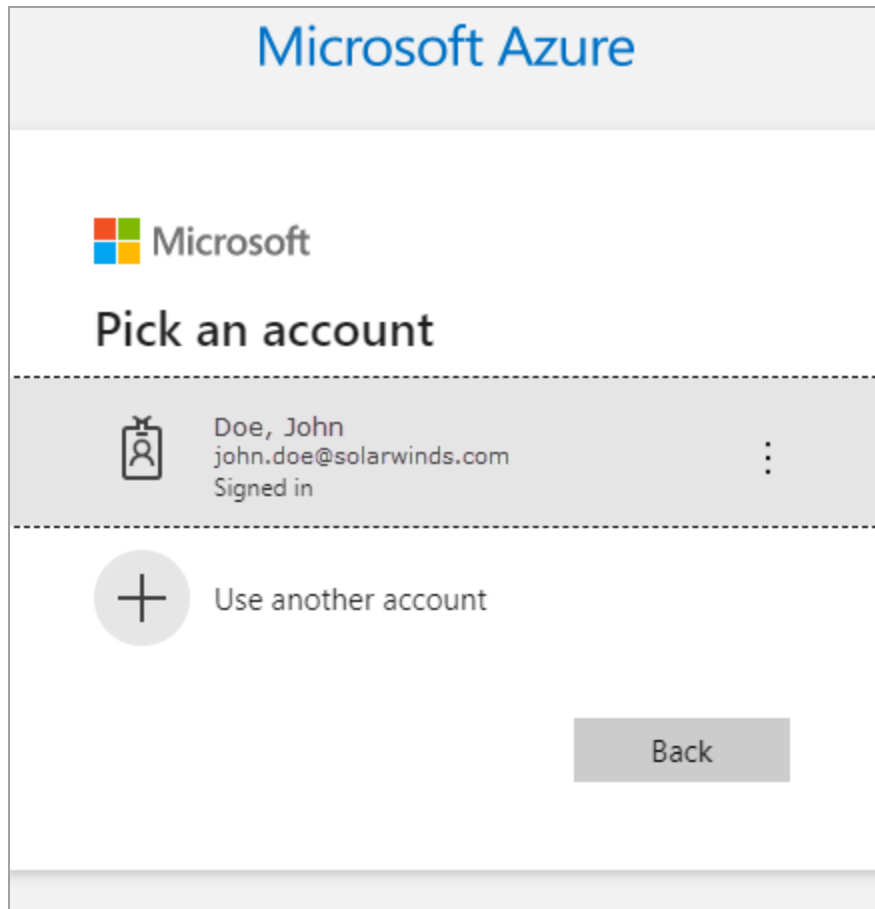
3. From a command line (Windows Command Prompt or PowerShell), run the `az login` command.



A screenshot of a Windows Command Prompt window. The title bar reads "Command Prompt". The window content shows the following text: "Microsoft Windows [Version 10.0.16299.1451]" followed by "(c) 2017 Microsoft Corporation. All rights reserved." on the next line. The prompt "C:\Users\john.doe>" is followed by the command "az login".

 Log in with any authentication option. Running the `az login` command is recommended. For more details and other options, see [Sign in with Azure CLI 2.0](#) (© Microsoft 2023, available at learn.microsoft.com, retrieved March 20, 2023).

4. When the browser launches prompting you to log in, sign in to Microsoft Azure with your account credentials.




Create and manage storage accounts, resource groups, and locations

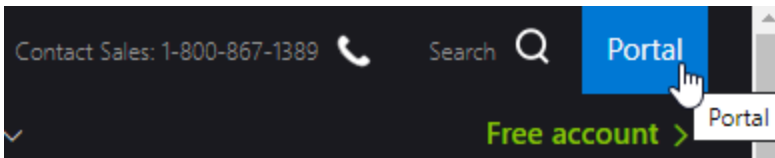
If you have a storage account, run the following command in the Azure CLI to display the account.

```
az storage account list
```

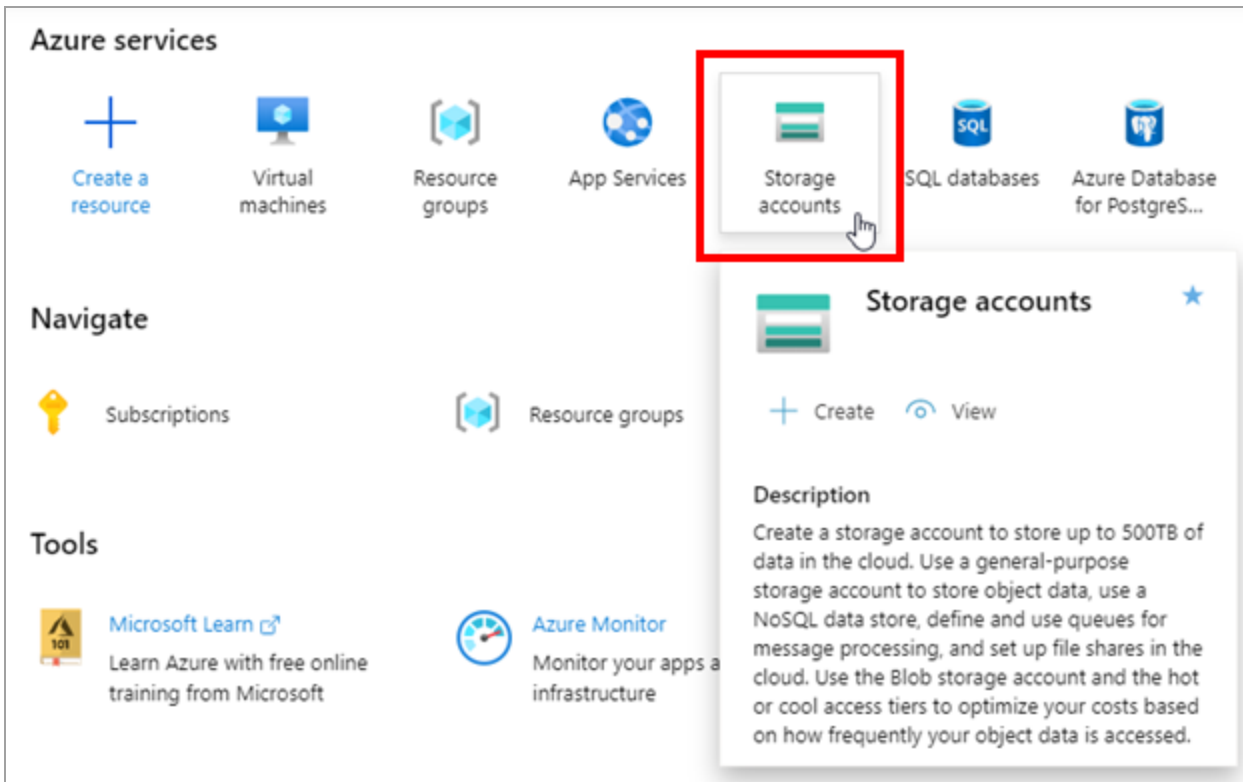
If a storage account does not exist, create a new account.

 The resource group name and location are in the JSON output. For details about listing the storage account in the command line, see [az storage account](#) on the Microsoft Learn website (© Microsoft Corporation, available at learn.microsoft.com, retrieved March 20, 2023).

To access the Azure Portal, click Portal in the upper right of the Microsoft Azure page.



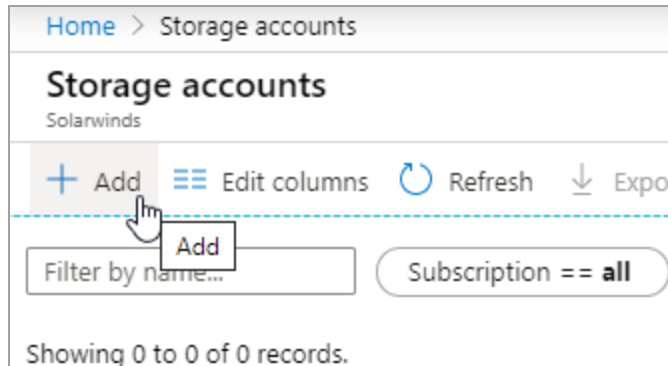
Storage accounts, locations, and resource groups are also available in the Azure Portal under Home > Storage accounts.



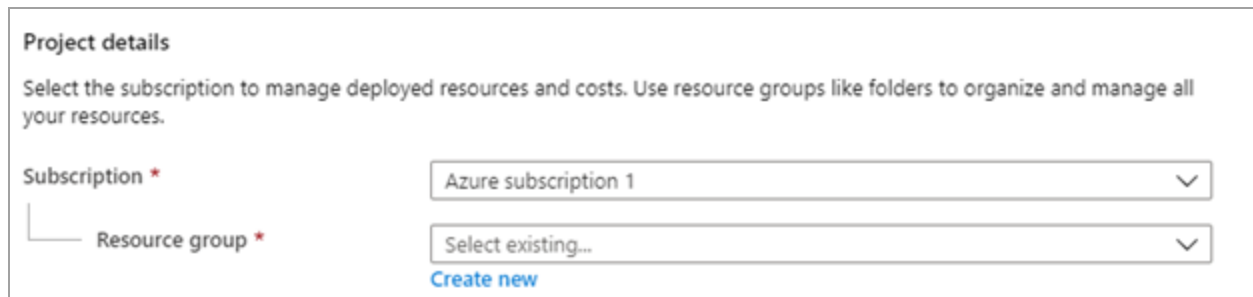
💡 The storage account name, location, and resource group names are required to run additional commands. Create and maintain a list for later use.

Create a storage account in the Azure Portal

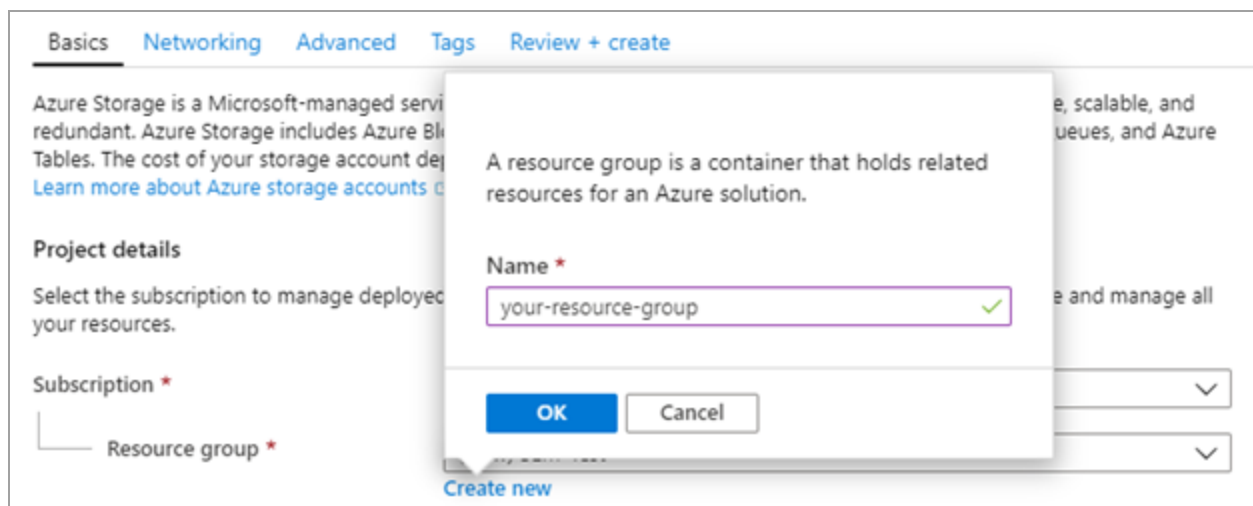
1. On the Azure Portal Home page, click Storage accounts.
2. On the Storage accounts toolbar, click Add.



3. Under Project details, select your Subscription and Resource group from the drop-down lists.



4. If you do not have a resource group, click Create new.



5. Enter a name for the resource group. **Record and save the name in a safe place.**
6. Click OK.

7. Under Instance details, enter a name for the storage account. **Record and save the name in a safe place.**

When you create a name, ensure that the name:

- Includes between 3 and 24 characters.
- Includes numbers and lowercase letters.
- Does not currently exist in Azure.

Instance details

The default deployment model is Resource Manager, which supports the latest Azure features. You may choose to deploy using the classic deployment model instead. [Choose classic deployment model](#)

Storage account name * ⓘ ✓

Location * ▼

Performance ⓘ ☒ Standard ☐ Premium

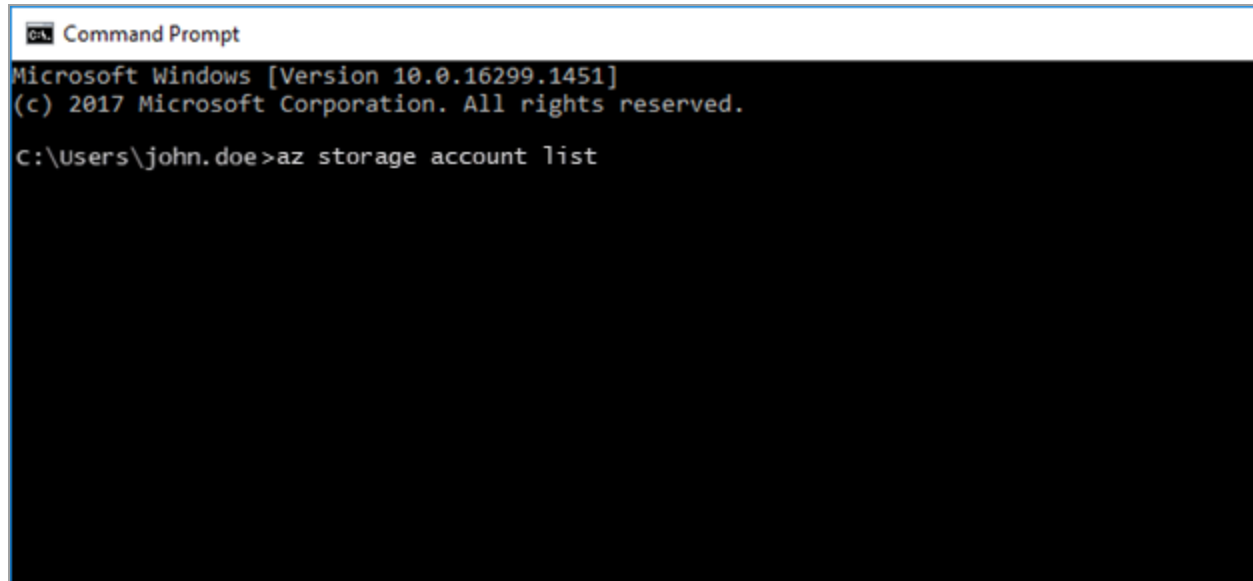
Account kind ⓘ ▼

Replication ⓘ ▼

Access tier (default) ⓘ ☐ Cool ☒ Hot

8. Select a location, or use the default location. **Record and save the location name in a safe place.**
9. Accept the default values for the remaining fields.
10. Click Review + create to review your settings, and then click Create.

11. To verify the storage account, open a command prompt and run the following command:

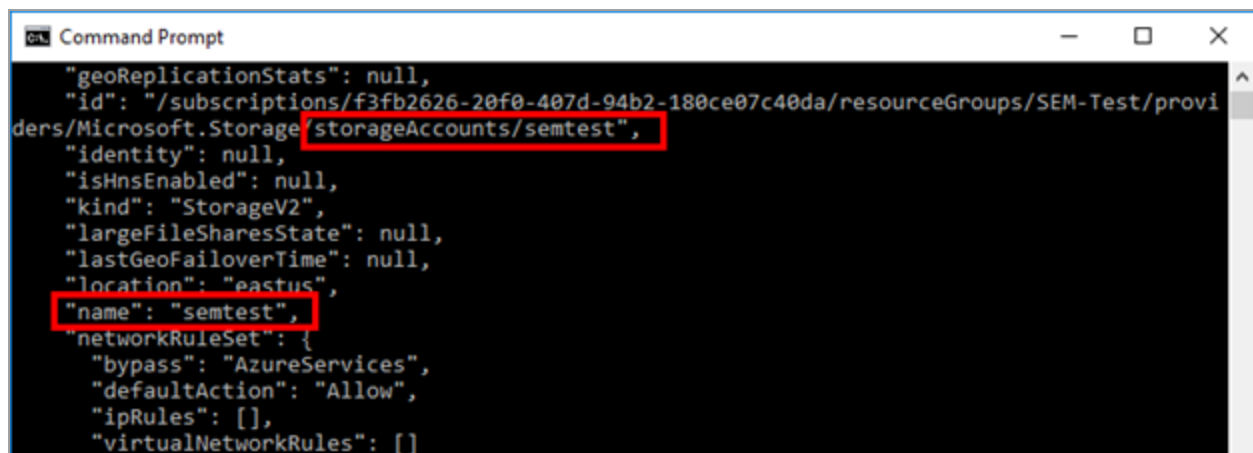


```
Command Prompt
Microsoft Windows [Version 10.0.16299.1451]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\Users\john.doe>az storage account list
```

where `john.doe` is your username.

12. Scroll down and locate the name of your new storage account.



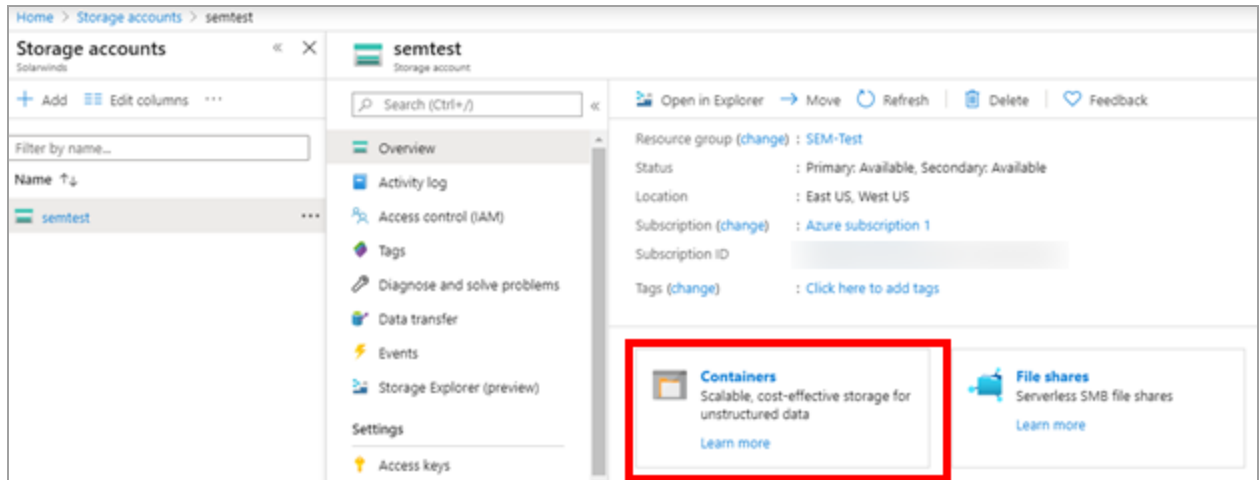
```
Command Prompt

{
  "geoReplicationStats": null,
  "id": "/subscriptions/f3fb2626-20f0-407d-94b2-180ce07c40da/resourceGroups/SEM-Test/provi
ders/Microsoft.Storage/storageAccounts/semtest",
  "identity": null,
  "isHnsEnabled": null,
  "kind": "StorageV2",
  "largeFileSharesState": null,
  "lastGeoFailoverTime": null,
  "location": "eastus",
  "name": "semtest",
  "networkRuleSet": {
    "bypass": "AzureServices",
    "defaultAction": "Allow",
    "ipRules": [],
    "virtualNetworkRules": []
  }
}
```



Record the names of your storage account and resource group, as well as the location. You will need them later.

13. Now that you have a storage account and resource group, create a container. The container holds your uploaded VHD files.
 - a. On the Azure Portal Home page, click Storage accounts.
 - b. Select your storage account, and then click Containers.



- c. On the Containers toolbar, click + Container.
- d. Enter a name for your container. **Record and save the name in a safe place.**
- e. Click OK.


Obtain a storage access key

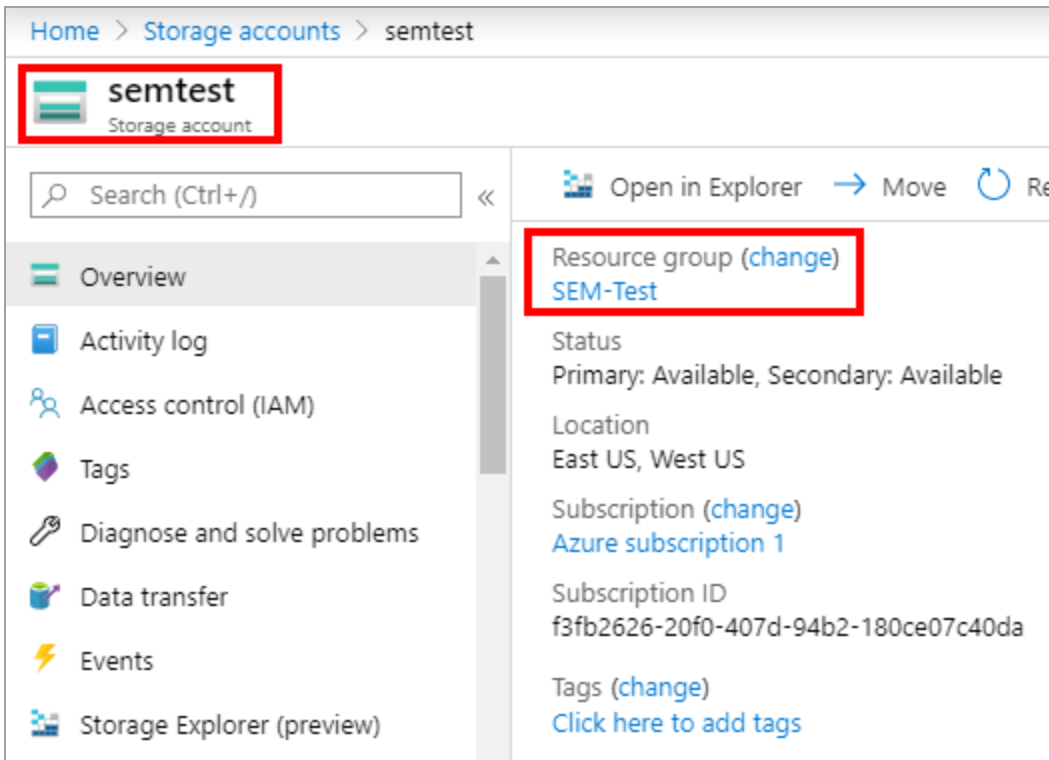
The storage account key is a 512b access key used to authenticate and access the storage account. The key is generated automatically when you create the storage account.

Enter the following command in the Azure CLI to list your storage account keys:

```
az storage account keys list --account-name <STORAGE_ACCOUNT> --resource-group <RESOURCE_GROUP>
```


where `STORAGE_ACCOUNT` and `RESOURCE_GROUP` are the storage account and resource group names you obtained in [Create and manage storage accounts, resource groups, and locations](#), respectively. You can find your storage account and resource group in the Azure Portal under Home > Storage accounts.

 Remove the angle brackets (< >) when entering the actual account and resource group names.

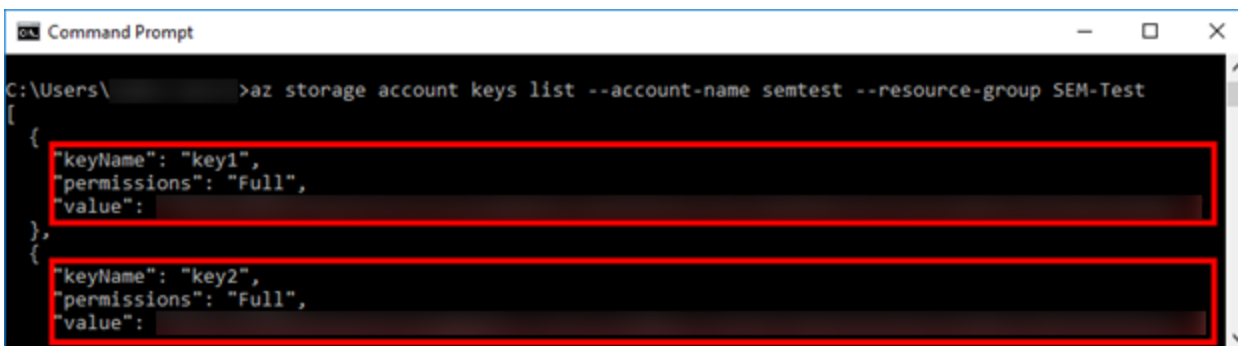


The command lists two storage account keys in JSON format:

- Primary (key1)
- Secondary (key2)

 JSON is the default format. You can change this format later.

You can use either key. For example:



```

C:\Users\>az storage account keys list --account-name semtest --resource-group SEM-Test
[
  {
    "keyName": "key1",
    "permissions": "Full",
    "value": "..."
  },
  {
    "keyName": "key2",
    "permissions": "Full",
    "value": "..."
  }
]

```

The screenshot shows a Windows Command Prompt window with the command `az storage account keys list --account-name semtest --resource-group SEM-Test` executed. The output is a JSON array containing two objects, each representing a storage account key. The first object has `"keyName": "key1"` and the second has `"keyName": "key2"`. Both have `"permissions": "Full"`. The `"value"` fields are redacted with ellipses. Red boxes highlight the JSON structure in the original image.

Prepare to deploy the virtual hard disks

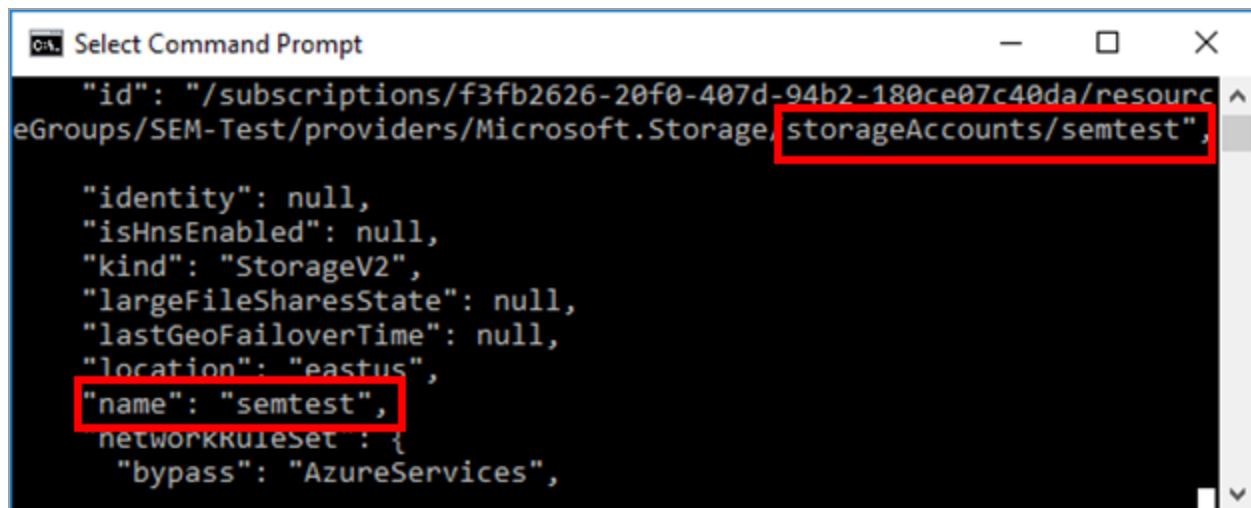
Before you deploy the virtual hard disks (VHDs), locate the following information you obtained in the following sections:

- [Create and manage storage accounts, resource groups, and locations](#)
- [Obtain a storage access key](#)

Each value stored in a variable in the following commands is typed as a token (for example, TOKEN), and should replace the code snippets below.

- Storage account name: STORAGE_ACCOUNT

Find your storage account name in the Azure Portal or run the `az storage account list` command, and then search for the storage account. In the example below, the storage account name is `semtest`.



```

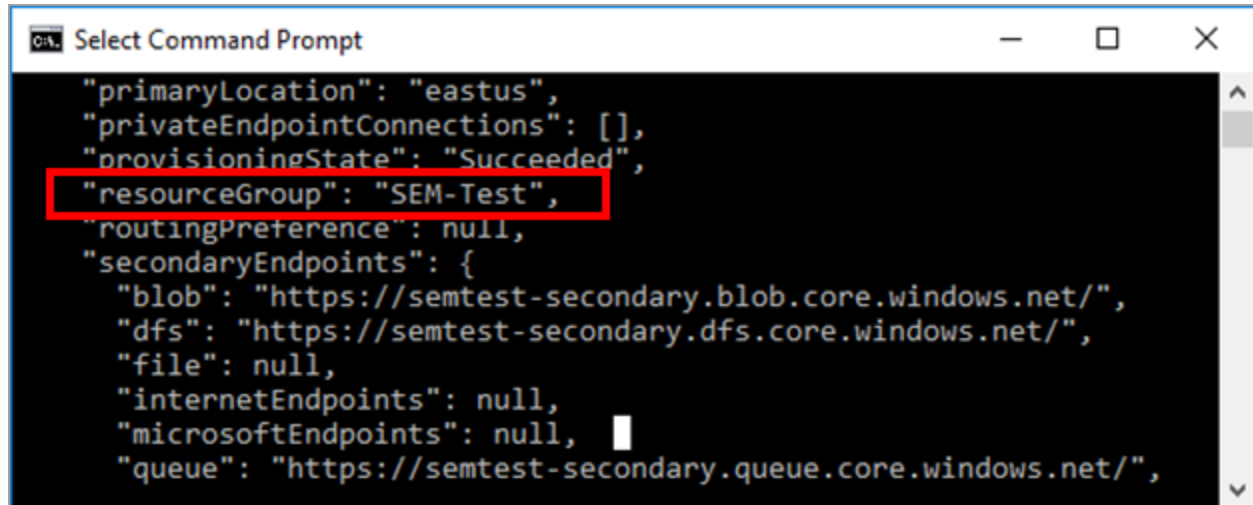
Select Command Prompt
{
  "id": "/subscriptions/f3fb2626-20f0-407d-94b2-180ce07c40da/resourceGroups/SEM-Test/providers/Microsoft.Storage/storageAccounts/semtest",
  "identity": null,
  "isHnsEnabled": null,
  "kind": "StorageV2",
  "largeFileSharesState": null,
  "lastGeoFailoverTime": null,
  "location": "eastus",
  "name": "semtest",
  "networkRuleSet": {
    "bypass": "AzureServices",

```

- Storage account key: [ACCESS_KEY](#)

- Resource group: RESOURCE_GROUP

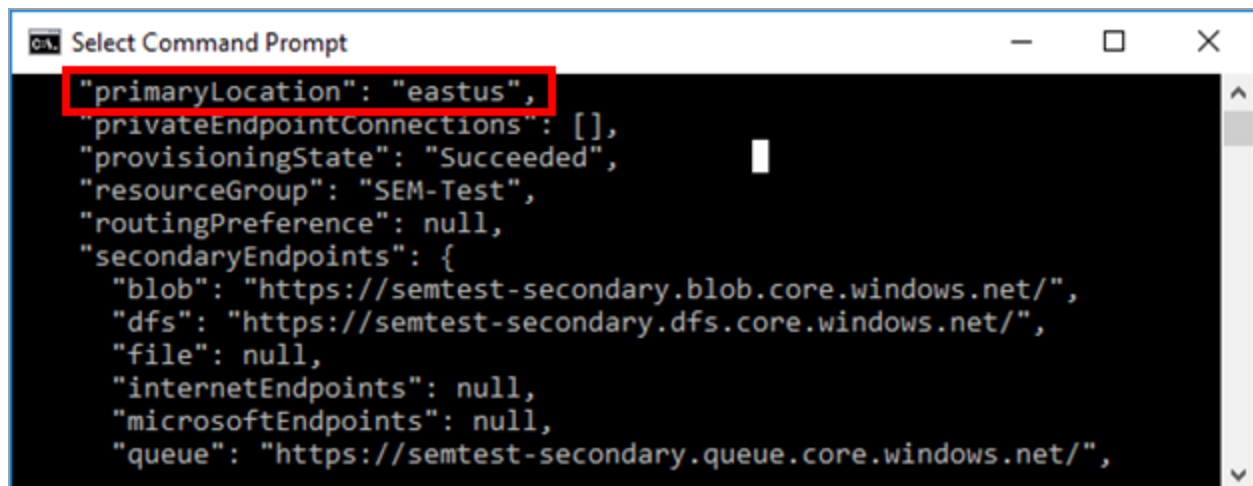
Find your resource group name in the Azure Portal, or run the `az storage account list` command, and then search for the resource group. In the following, the resource group is SEM-Test.



```
"primaryLocation": "eastus",
"privateEndpointConnections": [],
"provisioningState": "Succeeded",
"resourceGroup": "SEM-Test",
"routingPreference": null,
"secondaryEndpoints": {
  "blob": "https://semtest-secondary.blob.core.windows.net/",
  "dfs": "https://semtest-secondary.dfs.core.windows.net/",
  "file": null,
  "internetEndpoints": null,
  "microsoftEndpoints": null,
  "queue": "https://semtest-secondary.queue.core.windows.net/",
```

- Location: LOCATION

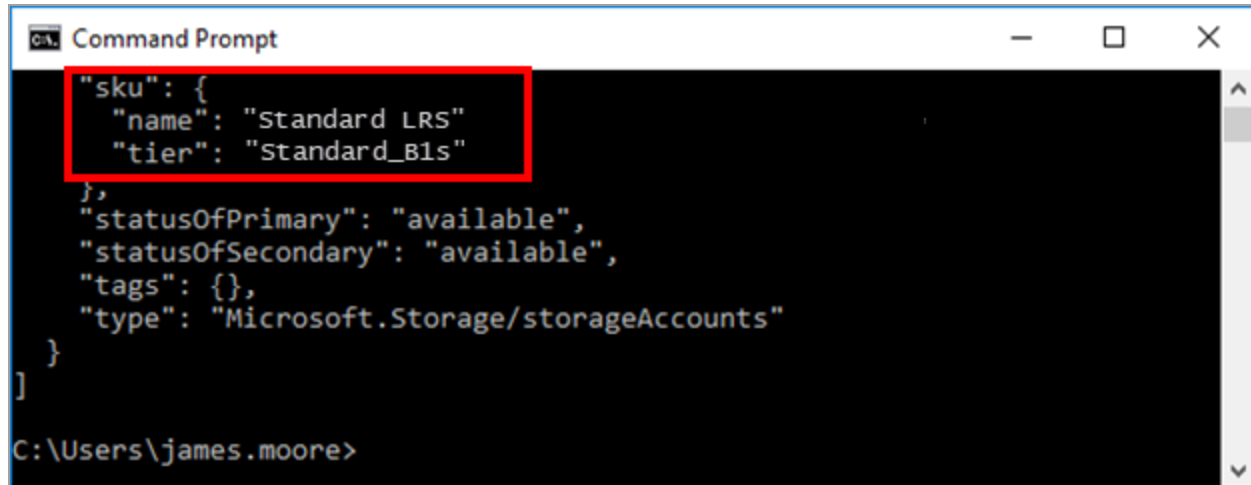
To find your location, look in your storage account details in the Azure Portal or run the `az storage account list` command, and then search for the location. In the following example, the location is `eastus`, for Eastern US.



```
"primaryLocation": "eastus",
"privateEndpointConnections": [],
"provisioningState": "Succeeded",
"resourceGroup": "SEM-Test",
"routingPreference": null,
"secondaryEndpoints": {
  "blob": "https://semtest-secondary.blob.core.windows.net/",
  "dfs": "https://semtest-secondary.dfs.core.windows.net/",
  "file": null,
  "internetEndpoints": null,
  "microsoftEndpoints": null,
  "queue": "https://semtest-secondary.queue.core.windows.net/",
```

- Storage size - sku: SKU

To find your sku, run the `az storage account list` command, and then search for the sku. In the example below, the sku name is `Standard_LRS`. The minimum requirement is `Standard_LRS`. Learn more about sku types [here](#) (© Microsoft 2020, available at learn.microsoft.com, retrieved October 5, 2020). If the returned SKU value is not supported (`Standard_RAGRS`, for example), change it to a supported value (see image below) when you update your script.




```

CA Command Prompt
{
  "sku": {
    "name": "Standard_LRS"
    "tier": "Standard_B1s"
  },
  "statusOfPrimary": "available",
  "statusOfSecondary": "available",
  "tags": {},
  "type": "Microsoft.Storage/storageAccounts"
}
]
C:\Users\james.moore>

```

- Virtual machine size: VM_SIZE

 To learn more about virtual machine sizing, see [Session virtual machine sizing guidelines](#) (© Microsoft 2023, available at learn.microsoft.com, retrieved on March 20, 2023). If you are missing anything from the list above, review the previous sections.

Additionally, the virtual machine name and disk names should be considered before deployment.

- Virtual machine name: VM_NAME

You can use any name you choose. For example, `solarwinds.sem`.

- Disk 1 (system) name: DISK1
- Disk 2 (data) name: DISK2

Enable the boot diagnostics

Boot diagnostics is a screen shot of the virtual machine video output. Enabling this feature is optional, but required before you [open a Support case](#) with SolarWinds Technical Support. The support representative will require the support key displayed in the screen shot.

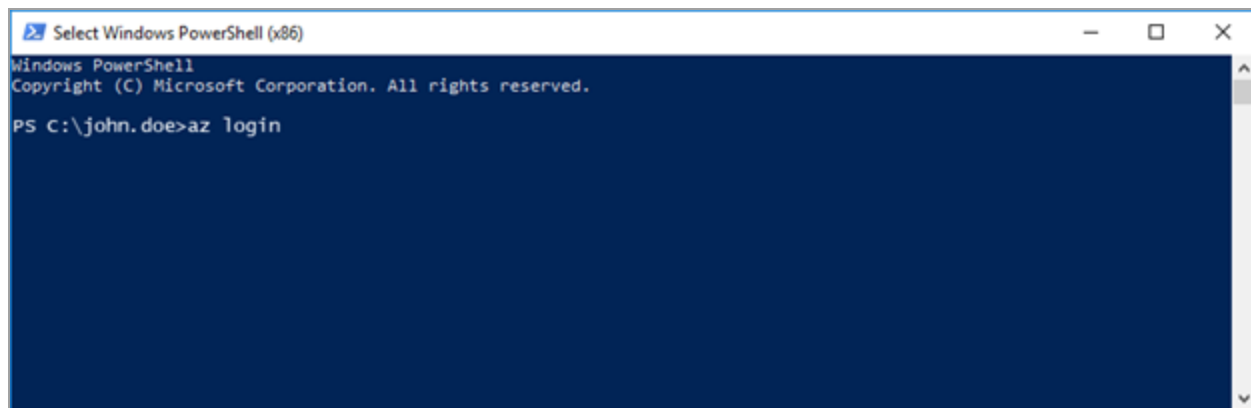
Deploy SEM from PowerShell (Windows)

i Scripts are not supported under any SolarWinds support program or service. Scripts are provided AS IS without warranty of any kind. SolarWinds further disclaims all warranties including, without limitation, any implied warranties of merchantability or of fitness for a particular purpose. The risk arising out of the use or performance of the scripts and documentation stays with you. In no event shall SolarWinds or anyone else involved in the creation, production, or delivery of the scripts be liable for any damages whatsoever (including, without limitation, damages for loss of business profits, business interruption, loss of business information, or other pecuniary loss) arising out of the use of or inability to use the scripts or documentation.

PowerShell is a command-line interface that is installed by default on the latest Microsoft systems. See [Windows PowerShell System Requirements](#) for details (© Microsoft 2023, available at [learn.microsoft.com](#), retrieved on March 20, 2023).

i Lines starting with the # character are comments. The back quote (`) character on the end of lines indicates multi-line commands.

1. Open a command prompt or PowerShell window.
2. From a command line, run the `az login` command.

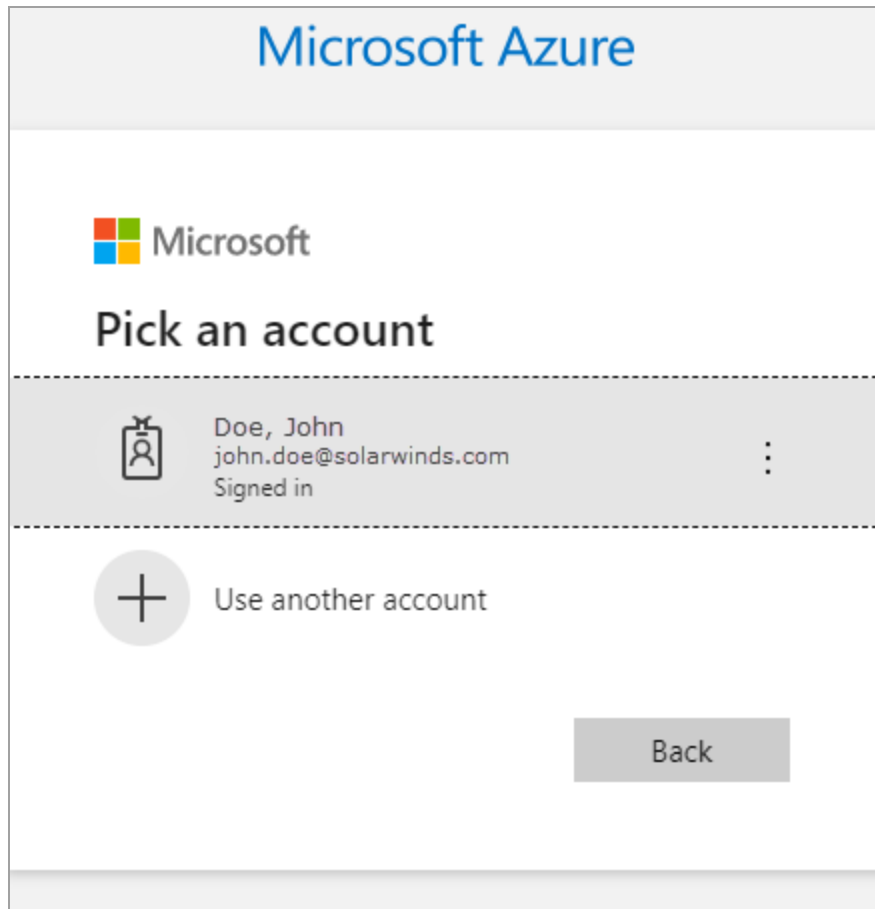


```
Select Windows PowerShell (x86)
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\john.doe>az login
```

i Log in with any authentication option. Running the `az login` command is recommended. For more details and other options, see [Sign in with Azure CLI 2.0](#) (© Microsoft 2022, available at [learn.microsoft.com](#), retrieved March 25, 2022).

3. When the browser launches prompting you to log in, sign in to Microsoft Azure with your account credentials.



4. Create your script.

The script will run, upload your two VHD files, and then create your VM in the Azure Portal. You can also download the script from SolarWinds using [this link](#).

The following script is a template. You will need to fill in the variables for your Azure VM environment.

```
<#Scripts are not supported under any SolarWinds support program or service.
Scripts are provided
AS IS without warranty of any kind. SolarWinds further disclaims all warranties
including,
without limitation, any implied warranties of merchantability or of fitness for a
particular purpose.
The risk arising out of the use or performance of the scripts and documentation
stays with you.
In no event shall SolarWinds or anyone else involved in the creation, production,
```

```
or delivery of the scripts be liable for any damages whatsoever(including, without
limitation,
damages for loss of business profits, business interruption, loss of business
information, or other
pecuniary loss) arising out of the use of or inability to use the scripts or
documentation
#>
# How to use:
# copy script to folder that contains azure disks
# change <SEM_VERSION>, <STORAGE_ACCOUNT>, <STORAGE_ACCESS_KEY>, <RESOURCE_GROUP>,
<VM_LOCATION>, <CONTAINER>
# log in to azure (az login)
# run script
#
#####

# storage account and key set to ENV to avoid typing it to each command
$env:AZURE_STORAGE_ACCOUNT="<STORAGE_ACCOUNT>"
$env:AZURE_STORAGE_KEY="<STORAGE_ACCESS_KEY>"

$container="<CONTAINER>"
$semVersion="<SEM_VERSION>"

Write-Host "SEM version: $semVersion" -foreground Green

$vmName="SEM-$semVersion"
$resourceGroup="<RESOURCE_GROUP>"
$sku="Standard_LRS"
$publicIpSku="Basic"
$vmSize="Standard_B1s"
$vmLocation="<VM_LOCATION>"
$osType="linux"

$disk1Filename="SolarWinds-SEM-Azure-$semVersion-disk1-system.vhd"
$disk2Filename="SolarWinds-SEM-Azure-$semVersion-disk2-data.vhd"

$disk1Name="$vmName-disk1.vhd"
$disk2Name="$vmName-disk2.vhd"

# check for presence of files
```

```
if (!((Test-Path $disk1Filename) -and (Test-Path $disk2Filename)))
{Write-Host "Couldn't find .vhd files" -foreground Red; break}

# upload system and data disks
az storage blob upload --container-name $container --type page --file
$disk1Filename --name $disk1Name
az storage blob upload --container-name $container --type page --file
$disk2Filename --name $disk2Name


# get blob urls
$blobUrlDisk1=az storage blob url --container-name $container --name $disk1Name
$blobUrlDisk2=az storage blob url --container-name $container --name $disk2Name

# create system and data disks
az disk create --resource-group $resourceGroup --sku $sku --name $disk1Name --
source $blobUrlDisk1
az disk create --resource-group $resourceGroup --size-gb "250" --sku $sku --name
$disk2Name --source $blobUrlDisk2

# create a machine and enable boot diagnostics
az vm create --resource-group $resourceGroup --size $vmSize --public-ip-sku
$publicIpSku --location $vmLocation
--name $vmName --os-type $osType --attach-os-disk $disk1Name
az vm disk attach -g $resourceGroup --vm-name $vmName --name $disk2Name

az vm boot-diagnostics enable --name $vmName --resource-group $resourceGroup --
storage $env:AZURE_STORAGE_ACCOUNT
```

5. Launch PowerShell.

 Change the directory (cd) in PowerShell to the directory where the VHD files reside on your local system.

```
PS C:\Users\ > cd C:\Users\ \Desktop\AzureDeployment
```

6. Paste your script into PowerShell, and then press Enter.

You can monitor the progress as the script is running. If the script encounters an error (such as a typo in your script), correct the error, and rerun the script.

When completed, you can access your new VM in the Azure Portal under Home > Virtual machines.

Deploy SEM from Bash (Linux)

i Scripts are not supported under any SolarWinds support program or service. Scripts are provided AS IS without warranty of any kind. SolarWinds further disclaims all warranties including, without limitation, any implied warranties of merchantability or of fitness for a particular purpose. The risk arising out of the use or performance of the scripts and documentation stays with you. In no event shall SolarWinds or anyone else involved in the creation, production, or delivery of the scripts be liable for any damages whatsoever (including, without limitation, damages for loss of business profits, business interruption, loss of business information, or other pecuniary loss) arising out of the use of or inability to use the scripts or documentation.

i Lines starting with the # character are just comments. The back quote (`) character on the end of lines is for multi-line commands.

1. Run Bash shell (WSL or native) where Azure CLI 2.0 is installed.
2. Log in to the Azure Portal.
3. Create your script.

The following script is a template. When you fill in the variables for your Azure VM environment, the script will run, upload your two VHD files, and then create your VM in the Azure Portal.

💡 Replace the values in red below with the values you recorded in the previous sections unless otherwise indicated. Enter values between the quotation marks, when present. Copy the entire script template into a text editor, such as Notepad, to make your edits.

```
# storage account and key set to ENV to avoid typing it to each command
$env:AZURE_STORAGE_ACCOUNT="STORAGE_ACCOUNT"
$env:AZURE_STORAGE_ACCESS_KEY="ACCESS_KEY"
$disk1Filename="SolarWinds-SEM-Azure-<SEM_VERSION>-disk1-system.vhd"
$disk2Filename="SolarWinds-SEM-Azure-<SEM_VERSION>-disk2-data.vhd"
$sku="Standard_LRS"
$vmSize="Standard_B1s"
$resourceGroup="RESOURCE_GROUP"
$vmLocation="LOCATION"

$disk1Name="SYSTEM-disk1.vhd"
$disk2Name="DATA-disk2.vhd"
$vmName="VM-NAME"

# upload system and data disks
```

```
az storage blob upload --container-name CONTAINER NAME --type page --file
$disk1Filename --name $disk1Name
az storage blob upload --container-name CONTAINER NAME --type page --file
$disk2Filename --name $disk2Name

# get blob urls
$blobUrlDisk1=az storage blob url --container-name CONTAINER NAME --name
$disk1Name
$blobUrlDisk2=az storage blob url --container-name CONTAINER NAME --name
$disk2Name

# create system and data disks
az disk create --resource-group $resourceGroup --sku $sku --name
$disk1Name --source $blobUrlDisk1
az disk create --resource-group $resourceGroup --size-gb "250" --sku $sku
--name $disk2Name --source $blobUrlDisk2

# create a machine and enable boot diagnostics
az vm create --resource-group $resourceGroup --size $vmSize --public-ip-
sku "Basic" --location $vmLocation --name $vmName --os-type "linux" --
attach-os-disk $disk1Name --attach-data-disks $disk2Name
az vm boot-diagnostics enable --name $vmName --resource-group
$resourceGroup --storage $env:AZURE_STORAGE_ACCOUNT
```

Below is an explanation of each value and variable. The first section below initializes the variables. The subsequent sections of the script will execute these variables to upload the disks and create the VM.

```
# storage account and key set to ENV to avoid typing it to each command
$env:AZURE_STORAGE_ACCOUNT="STORAGE_ACCOUNT" This is the resource group you created in the Azure Portal.
$env:AZURE_STORAGE_ACCESS_KEY="ACCESS_KEY" This is the multicharacter key you copied in a previous section. Paste the entire key between the quotation marks.
$disk1Filename="SolarWinds-SEM-Azure-<SEM_VERSION>-disk1-system.vhd"
$disk2Filename="SolarWinds-SEM-Azure-<SEM_VERSION>-disk2-data.vhd" The names of the system and data disk names will vary based on the SEM version. The system disk is much larger ~18GB - the data disk is typically ~1GB.
$sku="Standard_LRS" This is the minimum requirement.
$vmSize="Standard_B1s" This is the minimum requirement.
$resourceGroup="PROSCRIPTIVE" This is the resource group you created in the Azure Portal.
$vmLocation="LOCATION" For example, "eastus" for Eastern US.


$disk1Name="SYSTEM-disk1" You can give these disks any descriptive name you like.
$disk2Name="DATA-disk2"
$vmName="VM-NAME" You can give the VM any descriptive name you like.
```

The only other value you need to add is the container name you wrote down in a previous section as shown below. No quotation marks needed.

```
# upload system and data disks
az storage blob upload --container-name CONTAINER NAME --type page --file
$disk1Filename --name $disk1Name
az storage blob upload --container-name CONTAINER NAME --type page --file
$disk2Filename --name $disk2Name

# get blob urls
$blobUrlDisk1=az storage blob url --container-name CONTAINER NAME --name
$disk1Name
$blobUrlDisk2=az storage blob url --container-name CONTAINER NAME --name
$disk2Name
```

4. Launch Bash.

 Change the directory (cd) in Bash to the directory where the VHD files reside on your local system.

5. Paste your script into Bash, and then press Enter.

You can monitor the progress as the script is running. If the script encounters an error, such as a typo in your script, simply correct the error, and rerun the script.

When completed, you can access your new VM in the Azure Portal under Home > Virtual machines.

Deploy SEM on Amazon Web Services

To deploy SEM on Amazon Web Services (AWS):

1. [Prepare for the deployment.](#)
2. [Deploy AWS.](#)

See the [system requirements](#) for sizing, hardware, software, and port requirements.

 SolarWinds is not responsible for fees incurred when deploying SolarWinds products to AWS.

Prepare for the deployment

1. If you are an existing SEM user, contact [Customer Support](#) to request access to the AWS Amazon Machine Image (AMI) for SEM.

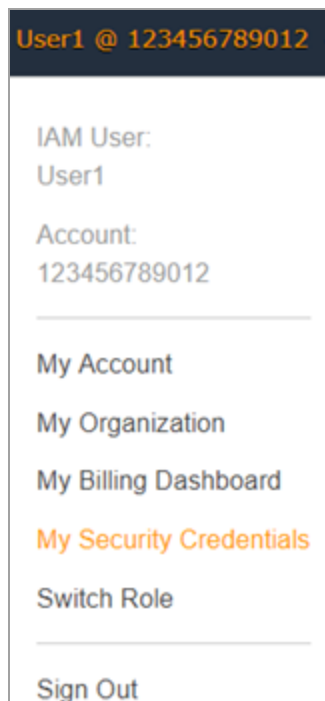
If you are evaluating SEM, contact your [SolarWinds Sales](#) representative to request access to the AWS AMI for SEM.

2. Locate your AWS account ID and AWS Region. You will need this information in a later step.
3. Verify that you have a copy of the PuTTY SSH client. You will need this utility in a later step.

 You can download PuTTY from the [PuTTY website](#).

4. Download, install, and configure the AWS Command Line Interface (CLI) for AWS account access.
5. Create and download an access key.

In the AWS Console, navigate to user menu > My Security Credentials > Create Access Key.

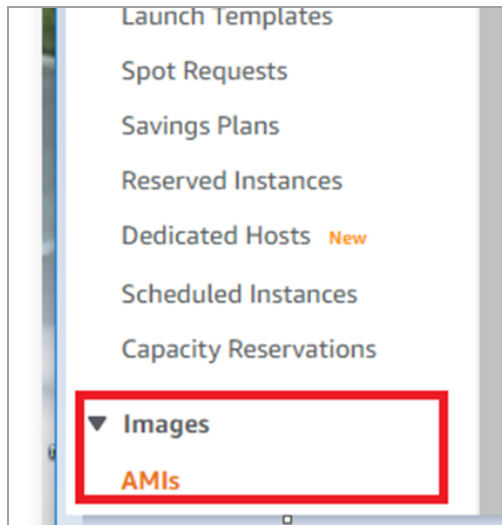


See [Managing access keys for IAM users](#) for details (© 2023 Amazon Web Services, Inc, available at docs.aws.amazon.com, retrieved March 20, 2023).

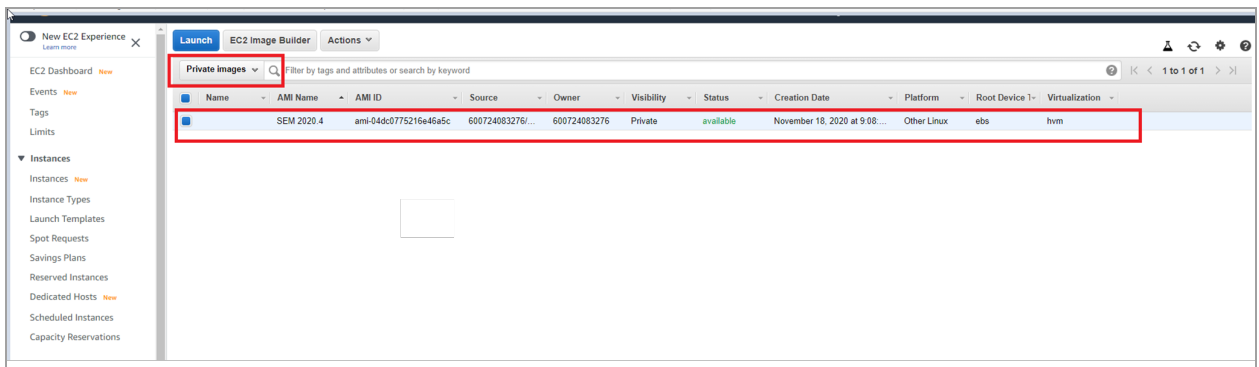
6. Save the access key ID and secret access key to a CSV file on your computer.

Deploy AWS

1. Verify that you have access to the AWS Amazon Machine Image (AMI) for SEM.
2. Locate your AWS account ID and AWS Region.
3. When you receive notification that your AMI is available, [launch the AMI](#) from the AWS EC2 console.
 - a. In the navigation menu, maximize Images and select AMIs.



- b. In the drop-down menu, select Private images.



- c. Select the SEM AMI, and then click Launch.
4. In the Choose an Instance Type page, select the instance type. Select at least t3.large, as this selection covers the default specifications for SEM.



SolarWinds recommends you use an instance type with an SSD if this is going to be a high volume deployment.

<input checked="" type="checkbox"/>	t3	t3.large	2	8	EBS only
-------------------------------------	----	----------	---	---	----------

5. Click Configure Instance.
6. In the Configure Instance Details window, adjust the allowed CPU as required. If you are using the recommended baseline 2 CPUs 8GB, do not select a CPU option that is less than this value.

1. Choose AMI
2. Choose Instance Type
3. Configure Instance
4. Add Storage
5. Add Tags
6. Configure Security Group
7. Review

Step 3: Configure Instance Details

Configure the instance to suit your requirements. You can launch multiple instances from the same AMI, request Spot instances to take advantage of lower prices, or use Reserved Instances for a lower price over the long term.

Number of instances
[Launch into Auto Scaling Group](#)

Purchasing option
☐ Request Spot instances

Network
[Create new VPC](#)

Subnet
[Create new subnet](#)

Auto-assign Public IP

Placement group
☐ Add instance to placement group

Capacity Reservation

Domain join directory
[Create new directory](#)

IAM role
[Create new IAM role](#)

CPU options
☐ Specify CPU options

Shutdown behavior

Stop - Hibernate behavior
☐ Enable hibernation as an additional stop behavior

Enable termination protection
☐ Protect against accidental termination

Monitoring
☐ Enable CloudWatch detailed monitoring
[Additional charges apply.](#)

Tenancy
[Additional charges will apply for dedicated tenancy.](#)

Elastic Inference
☐ Add an Elastic Inference accelerator
[Additional charges apply.](#)

Credit specification
☐ Unlimited

7. Click Add Storage.

The Add Storage window displays on your screen.

1. Choose AMI
2. Choose Instance Type
3. Configure Instance
4. Add Storage
5. Add Tags
6. Configure Security Group
7. Review

Step 4: Add Storage

Your instance will be launched with the following storage device settings. You can attach additional EBS volumes and instance store volumes to your instance, or edit the settings of the root volume. You can also attach additional EBS volumes after launching an instance, but not instance store volumes. [Learn more](#) about storage options in Amazon EC2.

Volume Type	Device	Snapshot	Size (GiB)	Volume Type	IOPS	Throughput (MB/s)
Root	/dev/sda1	snap-0f57eb38252614512	22	General Purpose SSD (gp2)	100 / 3000	N/A
EBS	/dev/sdb	snap-049b193cc390a	228	General Purpose SSD (gp2)	684 / 3000	N/A

[Add New Volume](#)

Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage. [Learn more](#) about free usage tier eligibility and usage restrictions.

8. In the Add Storage window, do the following:
 - a. Adjust the storage space, if required. Use the SSD options as they are needed to keep up with the amount of events being received by the SEM.
 - b. Modify `/dev/sdb` for additional log retention. You can change the disk size in the Size field if required.
9. Click Add Tags.
10. (Optional) If tags are part of your corporate policy, add a tag as required.

Step 5: Add Tags

A tag consists of a case-sensitive key-value pair. For example, you could define a tag with key = Name and value = Webserver. A copy of a tag can be applied to volumes, instances or both. Tags will be applied to all instances and volumes. [Learn more](#) about tagging your Amazon EC2 resources.

Key (128 characters maximum)	Value (256 characters maximum)	Instances	Volumes
This resource currently has no tags			
Choose the Add tag button or click to add a Name tag . Make sure your IAM policy includes permissions to create tags.			

[Add Tag](#) (Up to 50 tags maximum)

11. Click Configure Security Group.

The Configure Security Group window displays with the firewall policy for you syslog device and all agents.
12. Select Create a new security group, and then enter a security group name. For each firewall rule, enter the type, protocol, port range, source, and description.

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

Step 6: Configure Security Group

A security group is a set of firewall rules that control the traffic for your instance. On this page, you can add rules to allow specific traffic to reach your instance. For example, if you want to set up a web server and allow Internet traffic to reach your instance, add rules that allow unrestricted access to the HTTP and HTTPS ports. You can create a new security group or select from an existing one below. [Learn more](#) about Amazon EC2 security groups.

Assign a security group: ☒ Create a new security group ☐ Select an existing security group

Security group name:

Description:

Type	Protocol	Port Range	Source	Description
SSH	TCP	22	Custom 0.0.0.0/0	e.g. SSH for Admin Desktop

[Add Rule](#)

Warning
Rules with source of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.

13. Click Review and Launch.

14. In the Review Instance Launch window, review and verify your instance launch details.

Step 7: Review Instance Launch

Please review your instance launch details. You can go back to edit changes for each section. Click **Launch** to assign a key pair to your instance and complete the launch process.


Warning Improve your instances' security. Your security group, launch-wizard-1, is open to the world.

Your instances may be accessible from any IP address. We recommend that you update your security group rules to allow access from known IP addresses only. You can also open additional ports in your security group to facilitate access to the application or service you're running, e.g., HTTP (80) for web servers. [Edit security groups](#)

Warning Your instance configuration is not eligible for the free usage tier

To launch an instance that's eligible for the free usage tier, check your AMI selection, instance type, configuration options, or storage devices. [Learn more about free usage tier](#) eligibility and usage.

▼ AMI Details

 **SEM 2020.4 - ami-04dc0775216e46a5c**

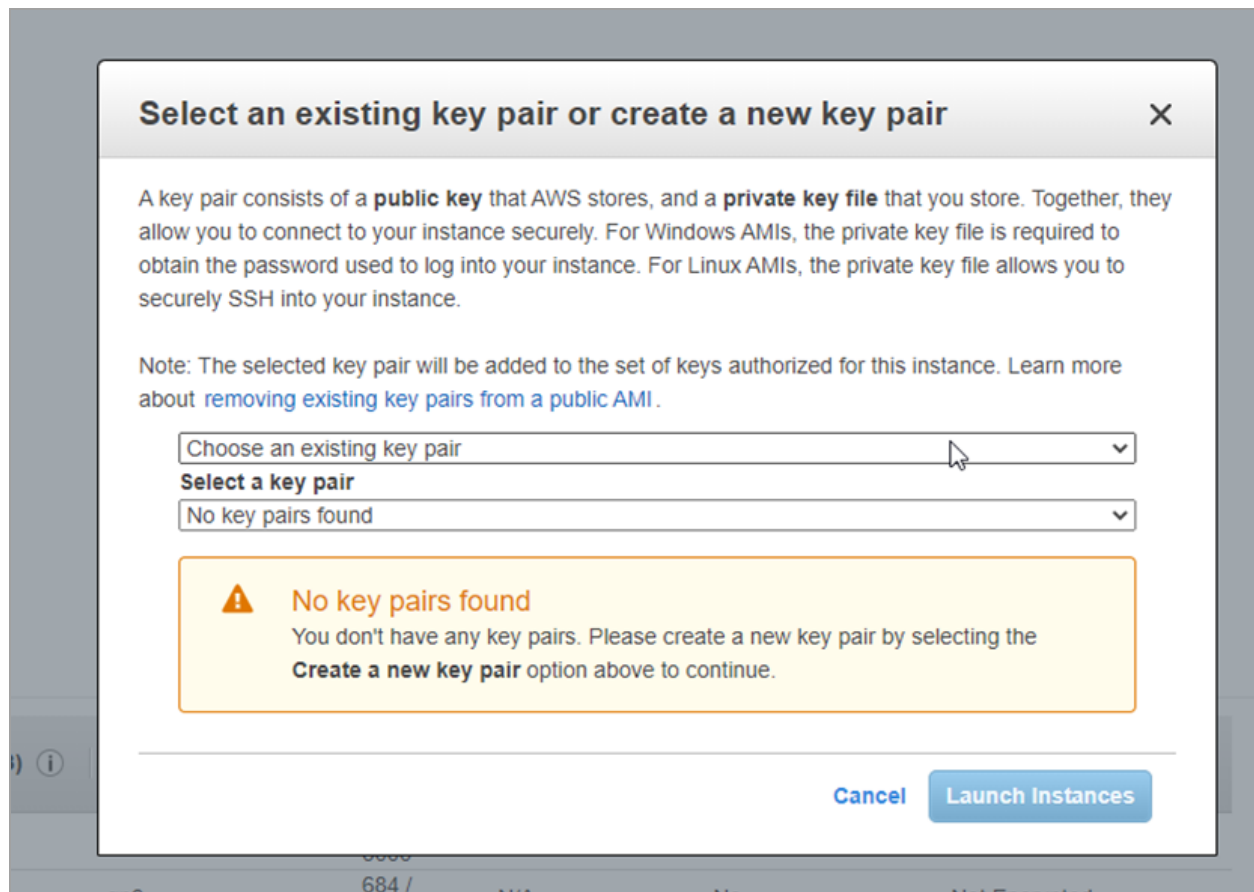
SEM 2020.4

Root Device Type: ebs Virtualization type: hvm

▼ Instance Type

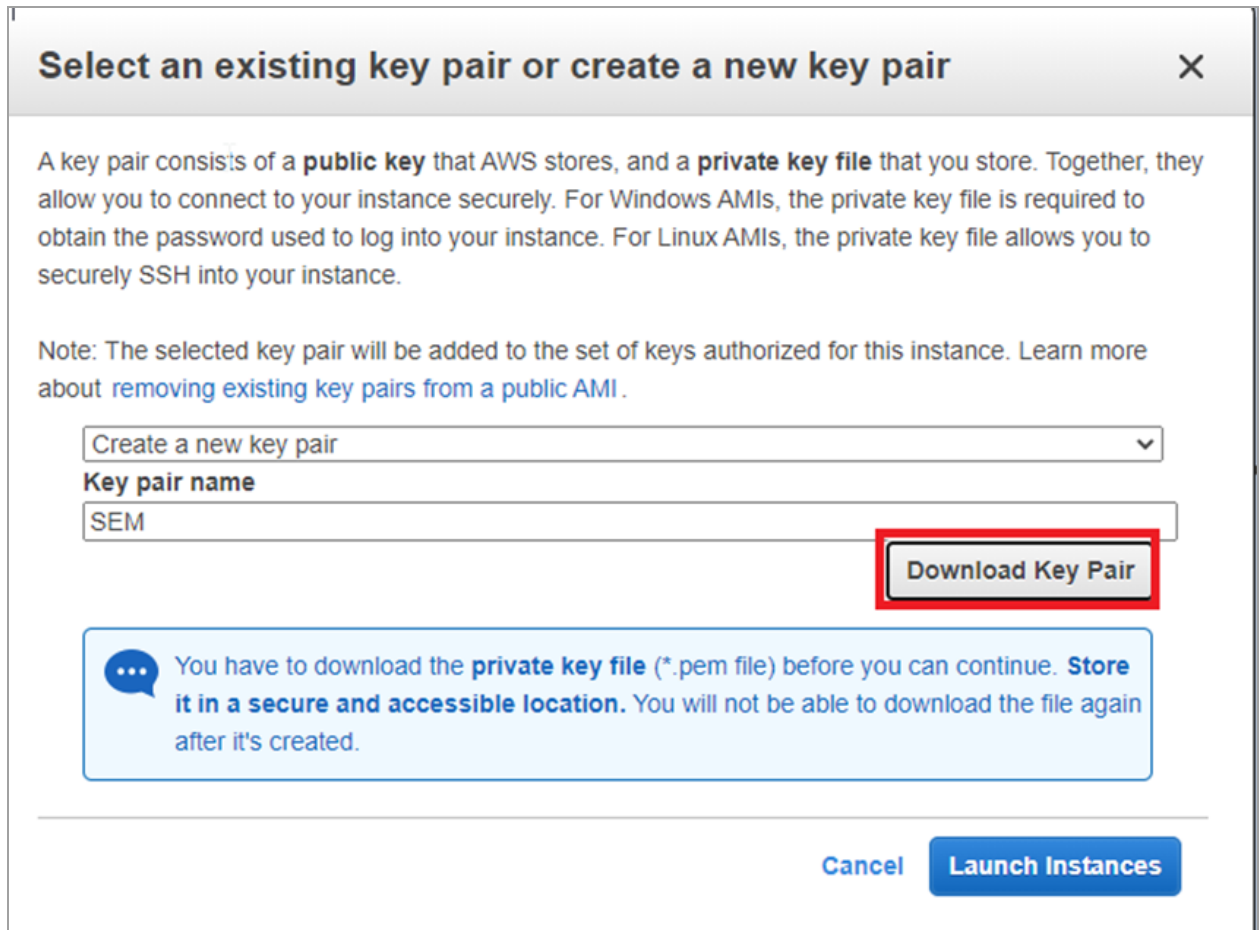
15. Click Launch to assign a keypair to your instance and complete the launch process.

16. Generate a key pair to connect using SSH to SEM.



(Screenshot © 2021, Amazon Web Services, Inc.)

- a. Click the first drop-down menu and select Create a new pair.



Select an existing key pair or create a new key pair X

A key pair consists of a **public key** that AWS stores, and a **private key file** that you store. Together, they allow you to connect to your instance securely. For Windows AMIs, the private key file is required to obtain the password used to log into your instance. For Linux AMIs, the private key file allows you to securely SSH into your instance.

Note: The selected key pair will be added to the set of keys authorized for this instance. Learn more about [removing existing key pairs from a public AMI](#).

Create a new key pair ▼

Key pair name

SEM

Download Key Pair

You have to download the **private key file** (*.pem file) before you can continue. **Store it in a secure and accessible location.** You will not be able to download the file again after it's created.

Cancel Launch Instances

(Screenshot © 2021, Amazon Web Services, Inc.)

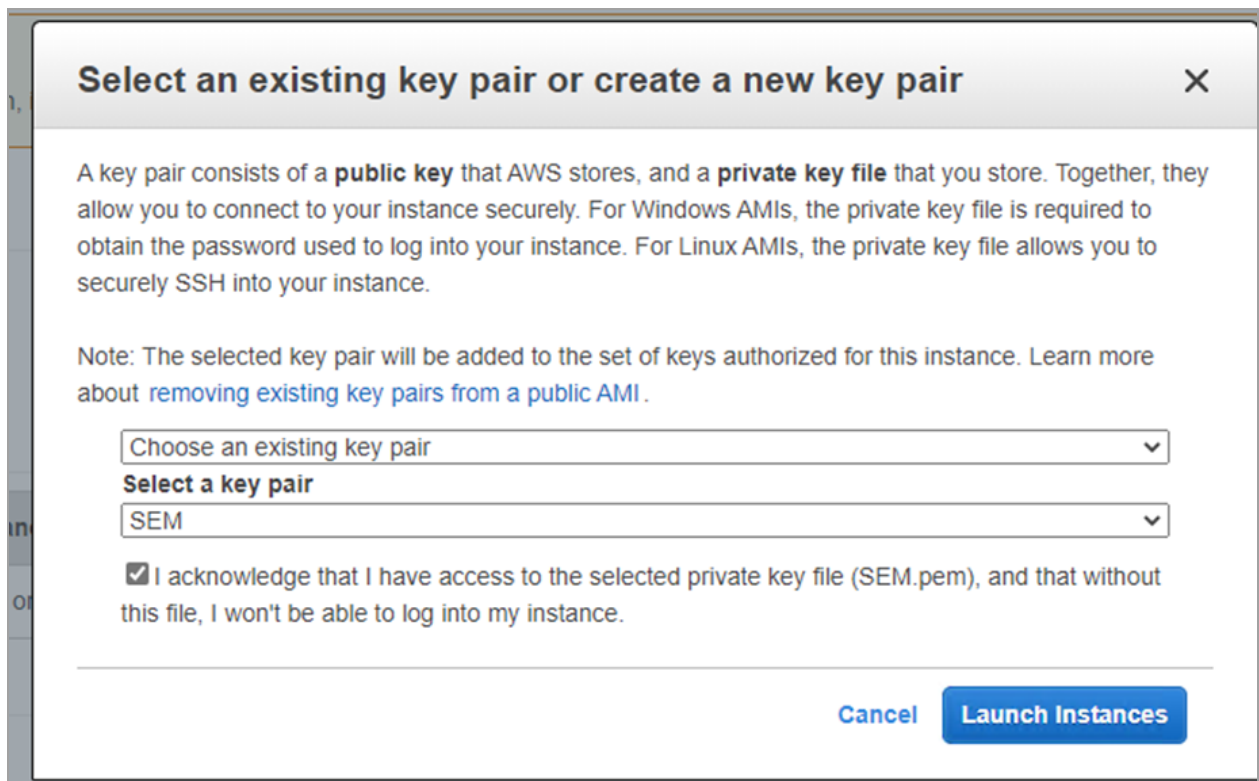
- b. In the Key pair name field, enter:

SEM

- c. Click Download Key Pair.
- d. Open PuTTY.
- e. Import the private key into PuTTY.

See [Connect to your Linux instance from Windows using PuTTY](#) from the [AWS Documentation](#) website for instructions.

- f. Select the checkbox to acknowledge that you have access to the selected private key file (SEM.pem). This is required to log in to your instance.



Select an existing key pair or create a new key pair ✕

A key pair consists of a **public key** that AWS stores, and a **private key file** that you store. Together, they allow you to connect to your instance securely. For Windows AMIs, the private key file is required to obtain the password used to log into your instance. For Linux AMIs, the private key file allows you to securely SSH into your instance.

Note: The selected key pair will be added to the set of keys authorized for this instance. Learn more about [removing existing key pairs from a public AMI](#).

Choose an existing key pair ▼

Select a key pair

SEM ▼

☒ I acknowledge that I have access to the selected private key file (SEM.pem), and that without this file, I won't be able to log into my instance.

Cancel Launch Instances


(Screenshot © 2021, Amazon Web Services, Inc.)

- g. Click Launch instances.

Complete the installation

After you run the SEM installer, do the following:

1. [Run the setup wizard.](#)
2. [Activate the SEM license.](#)
3. [Secure SEM from unauthorized users.](#)

 To prevent unauthorized access to your deployment, SolarWinds recommends that you avoid setting up the SEM appliance with access to the Internet or any public-facing network. See the [SEM security checklists](#) for additional security recommendations.

Run the setup wizard

After you [install and deploy SEM](#), run the setup wizard to accept the terms of the License Agreement and set up the default administrator credentials. When you are finished, you can [add additional SEM users](#) as needed.

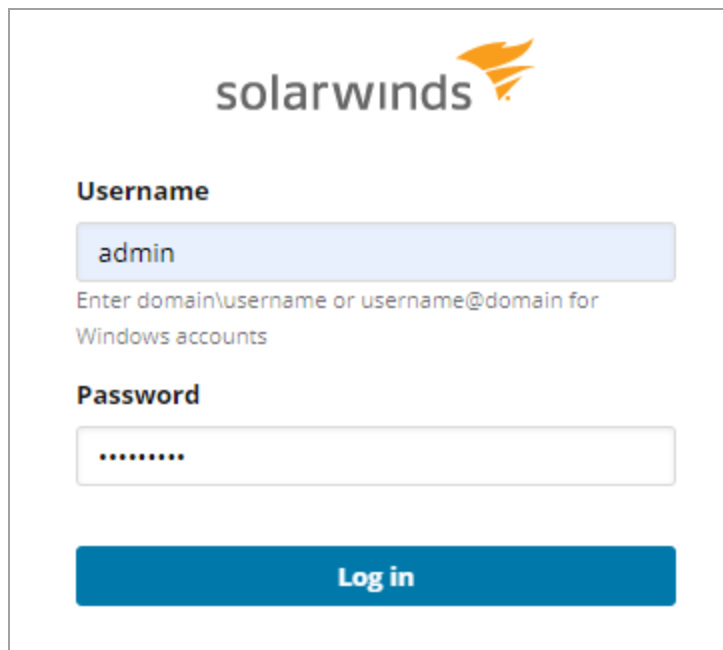
1. Open a [supported web browser](#).
2. Connect to the SEM Console.

In the address bar, enter the following URL and then press Enter:

`https://<appliance-ip-or-hostname>`

where <appliance-ip-or-hostname> is:

- The IP address or hostname of your Microsoft Hyper-V or VMware vSphere appliance you obtained when you [installed and deployed SEM](#)
 - The hostname of your Microsoft Azure, Azure CLI 2.0, or Amazon Web Services deployment you obtained when you [installed and deployed SEM](#)
3. In the SEM Console Login screen, click Log in to continue. The Username and Password fields are completed for you the first time you log in.



The login form features the SolarWinds logo at the top. Below it, the 'Username' section has a text input field containing 'admin' and a note: 'Enter domain\username or username@domain for Windows accounts'. The 'Password' section has a text input field with masked characters. A blue 'Log in' button is at the bottom.

solarwinds

Username


admin

Enter domain\username or username@domain for Windows accounts

Password

.....

Log in

 The default administrator username is `admin` and the password is `password`. You will be prompted to change your password after you log in for the first time.

4. If you accept the terms of the License Agreement, select the check box and then click Next.

Solarwinds SEM setup

License agreement

Change Password

Sign up for phoneho...

License agreement

IMPORTANT – READ CAREFULLY: BY DOWNLOADING, INSTALLING, AND/OR USING THE SOFTWARE (DEFINED BELOW), YOU (DEFINED BELOW) AGREE TO BE BOUND BY THE TERMS OF THIS AGREEMENT (DEFINED BELOW). IF YOU DO NOT AGREE TO THE TERMS OF THIS AGREEMENT, YOU MUST NOT DOWNLOAD, INSTALL, OR USE THE SOFTWARE, AND YOU MUST DELETE OR RETURN THE UNUSED SOFTWARE.

SOLARWINDS
END USER LICENSE AGREEMENT

This End User License Agreement (the "Agreement") is hereby entered into and agreed upon by you, either an individual or an entity, and its Affiliates (defined below) ("You" or "Company") and SolarWinds Worldwide, LLC ("SolarWinds Worldwide") for the Software (as defined below).

1. DEFINITIONS.

1.1 "Affiliates" means an entity controlled by, under common control with, or controlling such party, where control is denoted by having fifty percent (50%) or more of the voting power (or equivalent) of the applicable entity. Subject to the terms and conditions of this Agreement, Affiliates may use the license granted hereunder. All references to SolarWinds shall be deemed to be references to SolarWinds and its Affiliates, and all references to Company, You, or Your shall be deemed to be references to Company and its Affiliate(s).

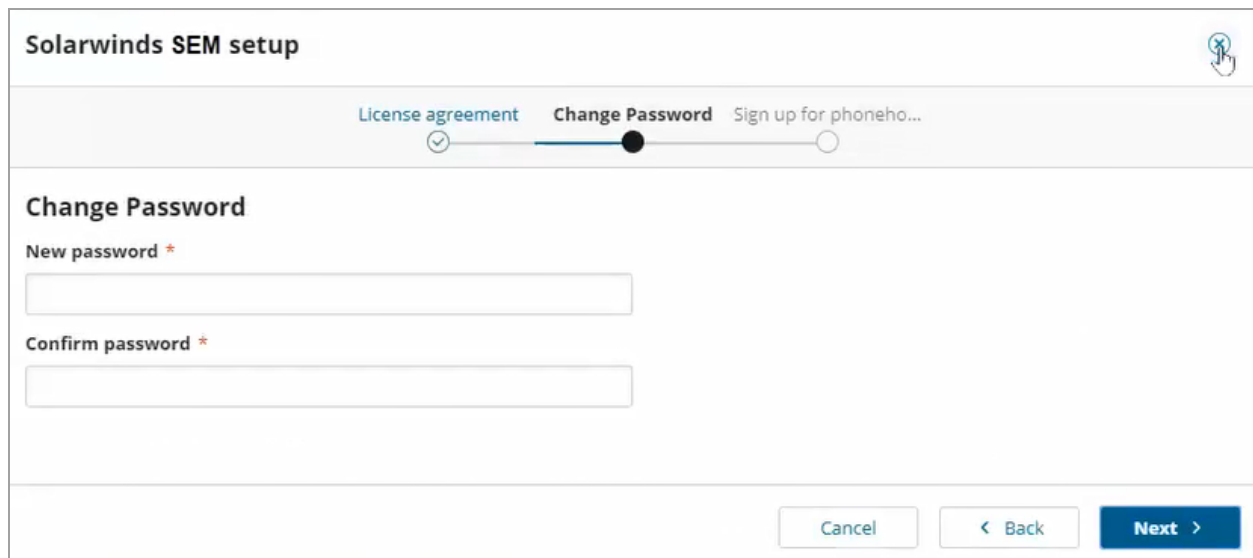
1.2 "Computer" means the hardware, if the hardware is a single computer system, whether physical or virtual, or means the computer system with which the hardware operates, if the hardware is a computer system component.

☒ I accept the terms of license agreement

Cancel

Next >

5. Create a new password using the following requirements:
 - Does not contain the word username.
 - Includes 6 to 40 characters.
 - Includes at least one uppercase letter.
 - Includes at least one lowercase letter.
 - Includes at least one digit.
6. Enter and confirm your new password, and then click Next.



Solarwinds SEM setup

License agreement ☒ **Change Password** ☒ Sign up for phoneho... ☐

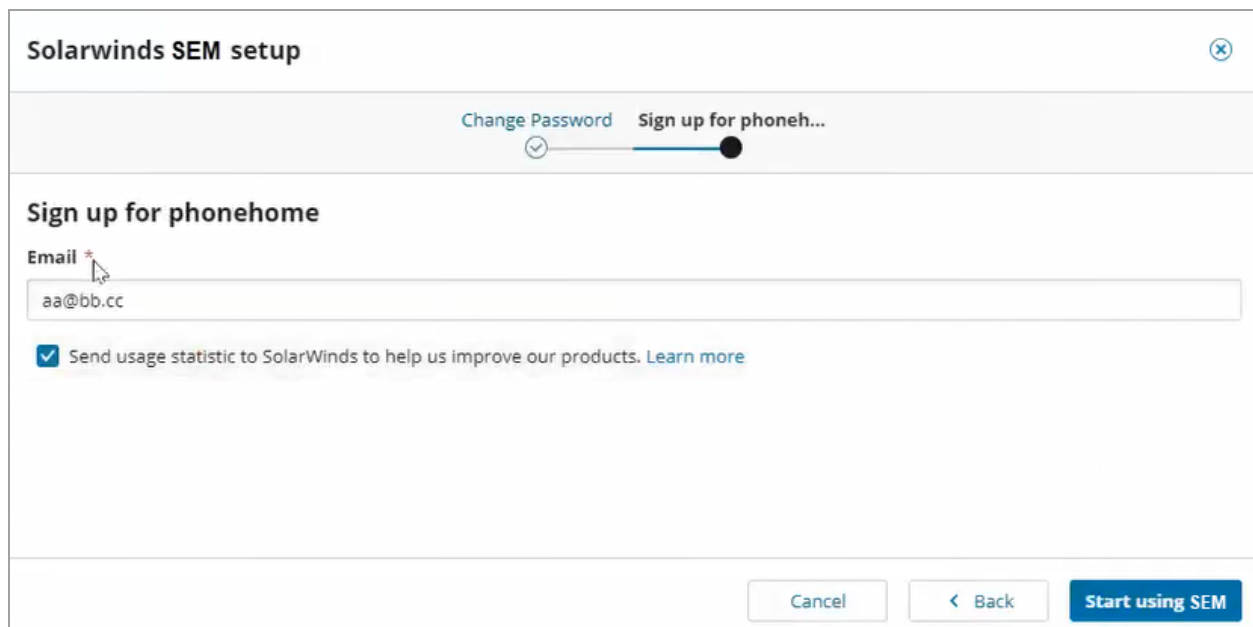
Change Password

New password *

Confirm password *

Cancel < Back **Next >**

7. Enter your email address for contact and download verification, and then select or clear the check box to send usage statistics to SolarWinds.



Solarwinds SEM setup

Change Password ☒ **Sign up for phoneh...** ☒

Sign up for phonehome

Email *

☒ Send usage statistic to SolarWinds to help us improve our products. [Learn more](#)

Cancel < Back **Start using SEM**

8. Click Start using SEM.

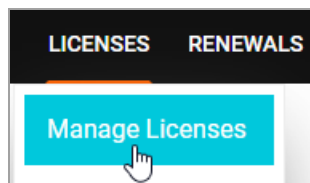
Activate the SEM license

After you [install and deploy SEM](#), activate your SEM license [online](#) or [offline](#).

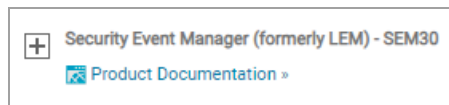
i If you [downloaded](#) and [installed](#) an evaluation, you can use SEM for 30 days. After 30 days, you must purchase and activate a license to continue using SEM in your environment.

Activate the license online

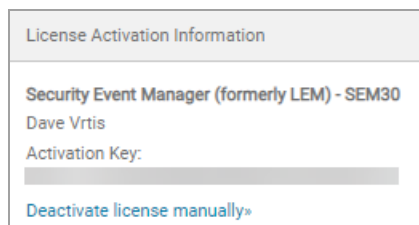
1. Log in to SEM as an administrator.
2. Open a separate browser window.
3. Navigate to the [SolarWinds Customer Portal](#).
4. Log in with your SolarWinds ID or individual user account and password.
5. Click Licenses > Manage Licenses.



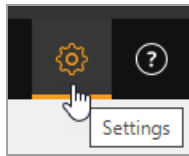
6. Scroll down to Security Event Manager (formerly LEM).



7. Click + to maximize the listing.
8. Under License Activation information, locate and copy the Activation Key to a safe location.

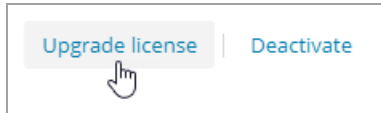


9. Log out of the Customer Portal.
10. Navigate back to SEM.
11. In the toolbar, click the Settings icon.

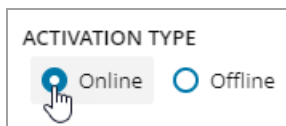


12. In the left column, click Manage License.

13. Click Upgrade license.



14. Under Activation Type, select Online.



15. In the License Key field, paste the license key that you copied from the Customer Portal.

License key

You can find your license key in Customer portal.

16. In the Name field, enter your name.

Name

17. In the E-mail field, enter your organization's email address.

Email

18. In the Phone number field, enter a contact phone number.

Phone number

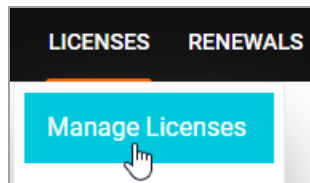
19. Click Activate.



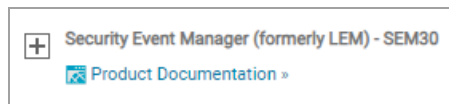
The license is activated.

Activate the license offline

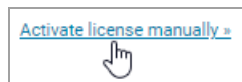
1. Log in to SEM as an administrator.
2. Open a separate browser window.
3. Navigate to the [SolarWinds Customer Portal](#).
4. Log in with your SolarWinds ID or individual user account and password.
5. Click Licenses > Manage Licenses.



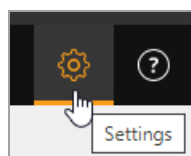
6. Scroll down to Security Event Manager (formerly LEM).



7. Click + to maximize the listing.
8. Under License Activation information, click Activate license manually.

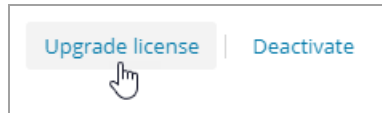


9. In the Manage License Activation page, complete the form entries, and then click Generate License File.
10. Save the license file to a network share that you can access from SEM.
11. Log out of the Customer Portal.
12. Navigate back to SEM.
13. In the toolbar, click the Settings icon.



14. In the left column, click Manage License.

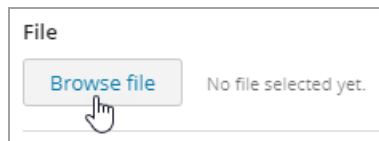
15. Click Upgrade license.



16. Under Activation Type, select Offline.



17. Click Browse file.



18. Navigate to the saved license file and select the file.

When you are finished, the Unique ID field populates with your license information.

19. Click Activate.



The license is activated.

Secure SEM from unauthorized users

After you [activate the SEM license](#), run the Activate command to help secure SEM from unauthorized users.

i You can still evaluate SEM without running the activate command. You can also turn off HTTP.

The activation procedure prompts you to:

- Configure a static IP address and hostname for the SEM VM
- Configure a secure password
- Verify your network configuration
- Export the SSL certificate that ensures secure communications between the SEM desktop console and the SEM Manager

i Port 8080 is unsecure and is automatically disabled after activation has been completed. Port 8443 is always available.

Prepare to run the Activate command

If you plan to use the SEM desktop console, copy the SEM CA SSL certificate to the Trusted Root Certification Authorities certificate store prior to running the Activate command.

i By default, SEM uses a pre-made, self-signed certificate.

When the activation is complete, the SEM VM automatically exports the SSL certificate. The SEM desktop console connects with the SEM Manager using secure communications on port 8443.

1. Open the CMC command line interface.

The default password is `password`.

See [Log in to the SEM CMC command line interface](#) for instructions.

2. At the `cmc>` prompt, type:

```
manager
```

3. Export the CA certificate so that you can import it into a computer running the SEM console.

At the `cmc : manager>` prompt, type:

```
exportcert
```

4. Follow the prompts to export the SEM Manager CA certificate.

An accessible network share is required. Once the export is successful, you will see the following message:

```
Exporting CA Cert to\\server\share\SWICAer -hostname.crt ... Success.
```

5. Locate and double-click the certificate on the network share.
6. Click Next.
7. Select Place all certificates in the following store, and then click Browse.
8. Select Trusted Root Certification Authorities.
9. Click OK, and then click Next.
10. Click Finish.
11. Click Yes to confirm that you trust the certificate.

Run the Activate command

1. Open the CMC command line interface.

The default password is `password`.

See [Log in to the SEM CMC command line interface](#) for instructions.

2. Configure SEM to use a static IP address.



SolarWinds recommends configuring a static IP address for the SEM VM. If you use DHCP instead and your IP address changes, your deployed Agents may be disconnected and require additional troubleshooting to resolve.

- a. At the `cmc>` prompt, type `appliance`, and then press Enter.

The prompt changes to `cmc::appliance>` to indicate that you are in the appliance configuration menu.

- b. Type `activate`, and then press Enter.

The Activation splash screen appears.

- c. Press Enter to go to the next screen.

- d. When prompted, select Yes to configure a static IP address for the SEM VM.

- e. At the `cmc::appliance>` prompt, type `netconfig`, and then press Enter.

- f. At the prompt, type `static`, and then press Enter.

- g. Follow the steps on your screen to configure the Manager Appliance network parameters.



Be sure to enter a value for each prompt. Leaving blank entries results in a faulty network configuration that requires you to rerun `netconfig`.

- h. Record the IP address assigned to the SEM VM. You will use this IP address to log in to the SEM console.

3. When prompted to change the hostname, select Yes to specify a hostname or No to accept the default hostname. To specify a hostname, use the following naming conventions:


- Hostname labels can only contain the following:
 - ASCII letters A through Z (letters are not case sensitive)
 - Digits 0 through 9
 - Hyphens (-)

- Hostnames cannot start with a digit or a hyphen, and must not end with a hyphen.
- No other symbols, punctuation characters, or white spaces are permitted.

4. Confirm your network configuration.

- a. At the `cmc::appliance>` prompt, enter:

```
viewnetconfig
```

 To ensure secure communications between SEM and the SEM desktop console, the SEM VM automatically exports an SSL certificate when the activation completes. Following activation, the SEM desktop console securely connects with the SEM VM on port 8443.

- b. Follow the prompts to export the certificate to a network share.

Install the SEM Agent

Install the SEM agent on the servers, domain controllers, and workstations you want to monitor in your organization.

SEM Agent deployment options

Review the options for deploying the SEM Agent to multiple Microsoft Window computers in an enterprise environment.

SolarWinds provides SEM agents for these operating systems:

- Microsoft Windows (local and remote installers)
- Linux
- Solaris on Intel
- Solaris on Sparc
- HPUX on Itanium
- AIX

The following table lists the installers you can use to deploy the SEM Agent non-interactively in a large Windows deployment.

Installer	Instructions
Remote Agent installer	See Run the SEM Remote Agent Installer .
Local Agent Installer with software distribution policies or local logon scripts	See Run the SEM Local Agent Installer .

You can install the Windows agents with an included Java Runtime Environment (JRE) or you can install the Windows agent and have it use the Java install on your system (customJava option).


See the release notes for the specific JRE version included with your SEM release.

See the [SEM Agent pre-installation checklist](#) for a list of tasks to complete before you install the SEM Agent.


SEM Agent pre-installation checklist

Before you install the SEM Agent, complete pre-installation checklist below. This checklist helps you:

- Gather the required credentials to complete the installation.
- Verify that system requirements are met and all required software is installed.

 See [SEM Agent deployment options](#) to learn about the options for deploying the agent.

SEM Agent installer requirements

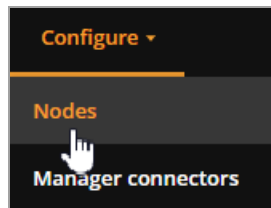
<input type="checkbox"/>	Review the system requirements	See the system requirements for details about the SEM Agent hardware and software requirements.
<input type="checkbox"/>	Gather the credentials	<p>Verify that you have administrative access to the servers and workstations you plan to monitor with the agent.</p> <p>Windows-based systems require Domain or Local administrative privileges. Linux or Unix systems require root-level access.</p> <div>  The Local Administrator account is not the same as a domain account with local admin rights. A domain account is subject to your domain group policies. </div>
<input type="checkbox"/>	Review the SEM Agent installation overview	See Deploy the SEM Agent installation overview for information about attended and unattended SEM agent installations.

Download the SEM Agent installers

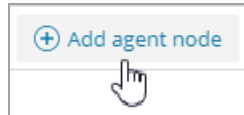
You can download SEM Agent installers from the SEM consoles or the [SolarWinds Customer Portal](#).

Download the installer from the SEM Console

1. Log in to the SEM Console.
2. In the SEM toolbar, click Configure > Nodes.




3. In the Nodes toolbar, click Add agent node.

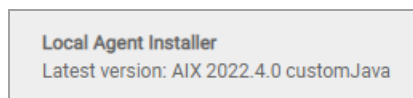


4. In the Add agent node window, follow the instructions to download the agent installer for a remote or local installation.

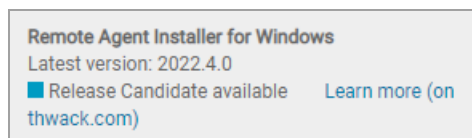
Download the installer from the SolarWinds Customer Portal

 If you are running a SEM evaluation, download the local or remote SEM Agent installer from the SEM Console or contact SolarWinds for assistance.


1. Log in to the [SolarWinds Customer Portal](#) with your SolarWinds ID (SWID).
2. Click Downloads > Download Product.
3. Click the Products drop-down menu and select:
Security Event Manager (SEM), formerly Log & Event Manager (LEM)
4. Click the Licenses drop-down menu and select a license option.
5. Scroll down to Agent Downloads.
6. Select a local agent installer for your product version.



or select a remote agent installer for your product version.



7. Click Download.
8. Follow the instructions on your screen to complete the download.

-  Before you deploy SEM agents, note the formatting in any .txt files that contain host entries:
- Ensure there is only one host entry per line.
 - If the format is tab separated, remove the tab spacing, and then enter a space between each value. For example, 10.10.10.10 xxx03 xxx03 yyy abcd.net. If tab spacing is present, the installer will not be able to parse the file correctly and will fail.


Install the SEM agents

See the following sections to install a SEM Agent:

- [Install the SEM Agent on Linux and Unix](#)
- [Run the SEM Remote Agent Installer](#)
- [Run the SEM Local Agent Installer](#)

Install the SEM Agent on Linux and Unix

Install the SEM Agent locally on a Linux and Unix operating system. When the installation is completed, the agent automatically starts and connects to SEM.

 See [SEM Agent pre-installation checklist](#) for agent download information and a pre-install checklist.

About the installation

By default, the SEM Agents are installed in the following folder:

`/user/local/contego/ContegoSPOP`

Download the SEM Agent installer

1. Log in to the [SolarWinds Customer Portal](#) using your SolarWinds ID (SWI).
2. Click Downloads > Download Product.
3. Click the Products drop-down menu and select Security Event Manager (SEM), formerly Log & Event Manager (LEM).
4. Click the Licenses drop-down menu and select your license tier.
5. Scroll down to Agent Downloads.
6. Click the Local Agent Installer drop-down menu, select a Linux release, and then click Download.
7. Review the message in the pop-up window, and then click Finish Download.

The installer is downloaded to your system.

For example:

```
SolarWinds-SEM-<version>-Agent-LinuxInstaller.bin
```

where `<version>` is the SEM release version.

For example:

```
SolarWinds-SEM-2023.2-Agent-LinuxInstaller.bin
```

Run the SEM Agent installer on Linux or Unix

1. Copy the installer file to a local or network location.
2. Open a Terminal window.
3. Change directories to the folder that contains the installer.
4. In the Terminal window, enter the following command to convert the installer into an executable application.

```
chmod +x SolarWinds-SEM-<version>-Agent-LinuxInstaller.bin
```

where `<version>` is the SEM installer version you downloaded from the Customer Portal.

For example:

```
chmod +x SolarWinds-SEM-2023.2-Agent-LinuxInstaller.bin
```

5. Run the following command as root:


```
./SolarWinds-SEM-Agent-<version>-LinuxInstaller.bin
```

For example:

```
./SolarWinds-SEM-Agent-2023.2-LinuxInstaller.bin
```

6. Press Enter to start the installer.
7. Press Enter to page through the End User License Agreement. If you agree with the agreement, enter `y` to accept the terms.
8. Enter a custom installation path or press Enter to accept the default (recommended).

9. Enter the hostname or IP address of the SEM Manager.

 Use the fully qualified domain name for your SEM Manager when you deploy SEM agents on a different domain. For example, enter `SEMhostname.example.com`.

10. Press Enter twice to accept the default port values, and then press Enter again to proceed.
11. Review the Pre-Installation Summary, and then press Enter.
12. After the installation is completed, press Enter to exit the installer.

The SEM Agent begins sending alerts to SEM.

If you need to install the agent on additional servers, see [Install the Linux \(or Unix\) agent on multiple servers](#) for instructions.

Next steps:

- See [Verify the SEM Agent connection](#) to test that the agent connected to the SEM Manager.

Uninstall the SEM Agent on Linux or Unix

1. Log in to your Linux system as root.
2. Stop the SolarWinds SEM Agent service.
3. Delete the `/usr/local/contego/ContegoSPOP` folder.
4. Remove any startup scripts.

The SEM Agent is uninstalled.

Download the SEM Agent for Windows

The Windows Agent installer allows you to install SEM agents locally on a variety of Windows operating systems. When the installation is completed, the SEM agent automatically starts and connects to your SEM Manager.

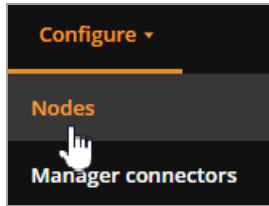
Download the SEM Agent installer

If you are running a SEM evaluation, [download the installer for an unlicensed SEM evaluation](#) or [contact SolarWinds Support](#) for assistance.

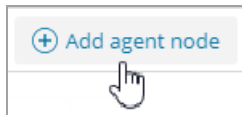
If you are running a licensed SEM version, [download the installer for a licensed SEM version](#).

Download the installer for an unlicensed SEM evaluation

1. Log in to the SEM Console as an administrator.
2. In the SEM toolbar, click Configure > Nodes.



3. In the Nodes toolbar, click Add agent node.



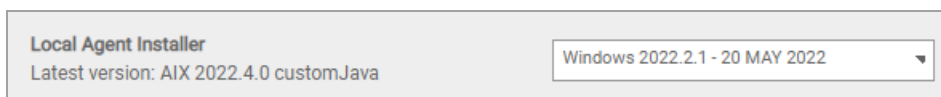
4. Click the Windows agent installer for a remote or local installation, based on your environment.

Download the installer for a licensed SEM version

1. Log in to the [SolarWinds Customer Portal](#) using your SolarWinds ID (SWI).
2. Click Downloads > Download Product.
3. Click the Products drop-down menu and select:
Security Event Manager (SEM), formerly Log & Event Manager (LEM)
4. Click the Licenses drop-down menu and select your license tier.
5. Scroll down to Agent Downloads.
6. Select and download the local or remote agent installer based on your deployment requirements.

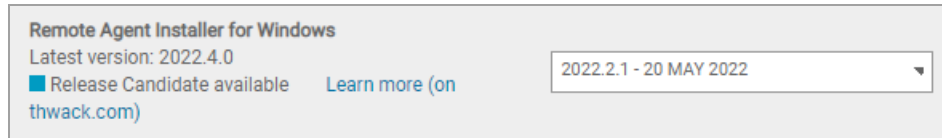
If you are installing the agent locally, locate the Local Agent Installer. Click the product version drop-down menu, select the targeted SEM version for your Windows operating system, and then click Download.


For example:



If you are installing the agent(s) remotely, locate the Remote Agent Installer for Windows. Click the product version drop-down menu, select the targeted SEM version for your Windows operating system, and then click Download.

For example:



 If a Release Candidate is available, this information displays in the selection.

7. If prompted, click Finish Download.

The installer is downloaded to your system.

For example:


`SolarWinds-SEM-<version>-Agent-WindowsInstaller.zip`

where `<version>` is the SEM release version.

For example:

`SolarWinds-SEM-2022.4-Agent-WindowsInstaller.zip`

Run the SEM Agent installer

 If you are upgrading the SEM Agent to the latest version, [uninstall the existing SEM Agent](#) first before you run the new installer.

For remote agent installations, see [Run the SEM Remote Agent Installer](#).

For local agent installations, see [Run the SEM Local Agent Installer](#).

SEM agents installed on SEM 6.7 and newer

In SEM 6.7 and newer, corresponding agent versions communicate by default using a secure certificate, which no longer requires TLS 1.0, 3DES, or anonymous cipher.

If you need to connect to earlier agent versions, navigate to the SEM Console security tab (Settings > Security), and switch the toggle button to enable lower security settings.

Run the SEM Remote Agent installer

The Remote Agent Installer allows you to install the SEM Agent on multiple Windows computers without the need to step through an installation wizard. When the installation is completed, the SEM Agent automatically starts and connects to the SEM Manager.

 See the [SEM Agent pre-installation checklist](#) for agent download information and a pre-installation checklist.

About the installation

The remote agent installer only applies to systems running Windows. You must have a user account with privileges to write to Windows administrative shares, such as C\$ or D\$.

The SEM agents are installed to the following locations, based on the system processor speed:

Processor	Installation folder
32.bit	C:\Windows\system32\ContegoSPOP
64-bit	C:\Windows\sysWOW64\contegoSPOP

If you are installing SEM agents on the far end of a WAN link, copy the remote agent installer executable to the end of the link and run it at this location. This will avoid using your WAN bandwidth to copy SEM agents multiple times.


If NetBIOS is not enabled, the Remote Agent Installer will require a text file of available hosts with each IP address or hostname on its own line.

When the installation is completed, a reboot is not required.

Download the installer

See [Download the SEM Agent for Windows](#) for instructions.

Run the Remote Agent Installer for Windows

 If you are upgrading the SEM Agent to the latest version, [uninstall the existing SEM Agent](#) first before you run the new installer.

1. Extract the contents of the installer ZIP file to a local or network location.
2. Right-click the EXE file and select Run as administrator.

3. Click Next to start the installation wizard.
4. If you agree with the License Agreement, accept the agreement and then click Next.
5. Specify a temporary folder on your computer to use for the installation process, and then click Next.

The default location is:

```
C:\SolarWindsSEMMultiInstall
```

6. In the Manager Host field, enter the hostname of your SEM Manager. Do not change the default port values.

If you are deploying the SEM agents on a different domain, use the fully qualified domain name for your SEM Manager.


For example, enter:

```
SEMhostname.SolarWinds.com
```

7. Click Next.
8. Select Get hosts automatically or Get hosts from file (One host per line), and then click OK.

The following table provides a description of each option.

Option	Description
Get hosts automatically	Uses a NETBIOS broadcast to identify hosts on the same subnet and domain as the computer running the installer.


Option	Description
Get hosts from file (One host per line)	<p>Prompts you to select a text file with a list of hosts that require a SEM Agent.</p> <div> <p> The text file can contain hostnames, fully qualified domain names (FQDNs), or IP addresses, each on their own lines. If you plan to include DNS names, the computer running the installer must be able to resolve each DNS name.</p> </div> <p>Use this option if you are deploying SEM agents in one of the following network configurations:</p> <ul style="list-style-type: none"> • To computers that are not located on the same subnet as the host computer running the installer. The host computer may be able to access the different subnets, but their hosts will not be recognized by the NetBIOS broadcast used to automatically to obtain the hosts. • To a small segment of a large network, where choosing hosts from a list can be time prohibitive. • In a network with a complex naming scheme, where choosing hosts from a list can be time prohibitive.

9. Select the check boxes next to each computer that requires a SEM agent, and then click Next.
10. Confirm that the list is correct, and then click Next.
11. Specify the Windows destination for the remote installation. The default paths are provided for all supporting Windows systems.

SolarWinds recommends using the default paths. Windows may not recognize the SEM Agent as a service if the agent is not installed in a system folder.

By default, the installer automatically detects the host operating system. If the target hosts are running the same operating system. you can select a specific operating system.

12. Click Next.
13. Select the USB-Defender check box to install this software with the SEM Agent. Otherwise, clear the checkbox.

 SolarWinds recommends installing USB-Defender on all systems. USB-Defender will never detach a USB device unless you have explicitly enabled a corresponding rule. By default, USB-Defender generates alerts for USB mass storage devices attached to your SEM agents.

14. Click Next.
15. In the Pre-Installation Summary window, confirm the settings, and then click Install.
16. When the installation process is completed, click Next to start the SEM Agent service.
17. Inspect the Agent Log for any errors, and then click Next.
18. Click Done to exit the installer.

 A system reboot is not required.

The SEM Agent begins sending alerts to the SEM Manager. The SEM Agent continues running on your computer unless you uninstall or manually stop the SEM Agent service.

Next steps:

See [Verify the SEM Agent connection](#) to verify that the agent is connected to the SEM Manager.

Run the SEM Local Agent installer

The Local Agent installer can be used for attended or unattended (non-interactive) SEM Agent installations on a Windows system without the need to step through an installation wizard. When the installation is completed, the SEM Agent automatically starts and connects to the SEM Manager.

You can run the Local Agent installer using a software distribution policies or local logon scripts. This method is an alternative to the [SEM Remote Agent installer](#) used for large Windows deployment scenarios.

 This procedure applies to the local installer. Do not use the Remote Agent installer for this task.

About the installation

To install the SEM Agent using the Local Agent installer:

1. [Download the Local Agent Installer](#).
2. [Configure a custom installer properties file](#) that contains your environmental variables.
3. [Run the Local Agent Installer](#).

See the [SEM Agent pre-installation checklist](#) for agent download information and a pre-installation checklist.

See [Install Run the SEM Remote Agent installer](#) for more information about installing the SolarWinds SEM Agent.

Download the Local Agent installer

See [Download the SEM Agent for Windows](#) for instructions.

Configure a custom installer properties file


1. Open a text editor and create a file with the following two lines, followed by a carriage return:

```
MANAGER_IP=<SEMManagerHostname>
INSTALLER_UI=silent
INSTALL_USB_DEFENDER=<n>
```

where:

- *<SEMManagerHostname>* is the hostname or IP address of the SEM appliance.
- *silent* runs the installer in silent mode.
- *<n>* is 0 or 1. Enter 0 to not USB defender or 1 to install USB defender.

2. Verify that a blank line with a carriage return follows the `INSTALL_USB_DEFENDER` entry.

 A blank line with a carriage return after the `INSTALL_USB_DEFENDER` entry is required for the file to work correctly.

The file contents should display as follows:

```
MANAGER_IP=swi-sem
INSTALLER_UI=silent
INSTALL_USB_DEFENDER=0
```

3. Save the file as `installer.properties` in the same folder as the `.exe` file.

Run the Local Agent installer

1. Verify that `.exe` and `installer.properties` are located in the same folder.

 Do not use UNC paths during this installation.


2. Run the following command using the active resource directory that matches the folder with the two installation files:

```
setup -i silent
```

The command immediately returns to the command prompt.

3. Right-click the EXE installation file and select Run as administrator.

When the installation is completed, the SEM Agent begins sending alerts to your SEM Manager. The Agent runs on your system unless you uninstall or [stop the SEM Agent service](#).

 The SEM Agent should also display in Apps & features in your Windows operating system where you can remove the program (if required).

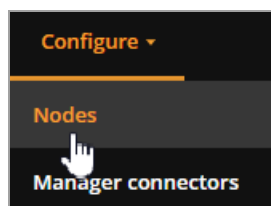
Next steps:

- See [Verify the SEM Agent connection](#) to test that the Agent connected to the SEM Manager.

Verify the SEM Agent connection

After you install the SEM Agent on your agent nodes using the SEM [Remote Agent](#) or [Local Agent](#) installer, verify that the agent is connected to the [SEM Manager](#).

1. Log in to the SEM Console as an administrator.
2. On the SEM toolbar, click Configure > Nodes.



3. In the left column under Refine results, click the Agent and Connected check boxes.
4. In the agent node list, ensure that all connected nodes display a green checkmark, as shown below.

See [Troubleshoot SEM agents and network devices](#) in the SEM Administrator Guide to troubleshoot the SEM agents.

- ### Next steps:

If you installed additional SEM agents, see [Create connector profiles to manage and monitor SEM agents](#) located in the SEM Administrator Guide for instructions.

Upgrade SEM

The Security Event Manager upgrade package upgrades SEM and the following components:

- SEM console
- SEM agents

To upgrade your SEM deployment, perform the following procedures:

1. [Determine the upgrade path](#) to the latest SEM version.
2. [Review the best practices](#) for SEM upgrades.
3. [Upgrade the SEM components](#).

Determine the SEM upgrade path

If you are running a SEM End of Life or End of Engineering version, you can update to the latest version by following the designated upgrade path for your version.

 If you need an upgrade package for an earlier LEM version or TriGeo SIM (which is no longer supported), [open a Customer Support ticket](#).

About the upgrade installers

Use the following installers to upgrade your deployment:

- Security Event Manager - Recovery Boot CD
- SEM Upgrade ISO

These installers are located on the [SolarWinds Customer Portal](#).

The **Security Event Manager - Recovery Boot CD** installer provides the necessary files to support older versions in the upgrade path. If you are running an End of Life or End of Engineering version, run the CD where indicated between each version in the upgrade path.

The **SEM Upgrade ISO** installer upgrades your deployment with a version you select and download in the Customer Portal. Based on the upgrade path, you may be required to download several versions of the SEM Upgrade ISO installer from the Customer Portal to upgrade your deployment to the latest release.

 See [Best practices for SEM Upgrades](#) for additional upgrade considerations.

Download the upgrade installers

1. Log in to the [SolarWinds Customer Portal](#).
2. Click Downloads > Download Product.
3. Click the Products drop-down menu and select:

Security Event Manager (SEM), formerly Log and Event Manager (LEM)
4. Click the Licenses drop-down menu and select your license tier.
5. Locate your current version listed in [Currently supported versions](#), [End of Engineering versions](#), or [End of Life versions](#).
6. Under Upgrade path, record the installers that are required to upgrade your deployment to the latest release.
7. If you are upgrading from SEM 2021.4 or earlier, download the Security Event Manager - Recovery Boot CD located under All Release Downloads. Otherwise, go to the next step.

Security Event Manager - Recovery Boot CD <small>Latest version: 2022.2.2</small>	2022.2.2 - 27 Oct 2022	 DOWNLOAD
--	------------------------	---

8. Download the SEM Upgrade ISO installer for your upgrade version.

For example, if you need to upgrade to version 2023.4.1 in the upgrade path, click the drop-down menu, select 2023.4.1, and download this installer.

SEM Upgrade ISO – this ISO can be used to upgrade your LEM appliance from 6.3.1 HF4 to 6.4 or from 6.4 to a newer version of SEM.	<div style="border: 1px solid #ccc; padding: 2px; display: inline-block;"> 2023.4.1 - 1 Mar 2024 ▼ </div>	 DOWNLOAD
---	---	---

9. Repeat step 8 for each additional installer required in the upgrade path, including the installer for the latest release.
10. [Upgrade the SEM components](#).

Example upgrade procedure

When you upgrade your SEM components from an existing version listed in the [Supported upgrade paths](#) table to the latest version, be sure to:

- Create a snapshot of each deployment in the upgrade path
- Ensure that:

- You can connect to the SEM Console.
- Your SEM deployment is functioning properly.
- All SEM Windows agents are upgraded, connected, and sending logs and events to the SEM Manager.

If you encounter issues during the upgrade, you can use a snapshot to revert to a previous version, fix any issues, and repeat the upgrade procedure.

The following procedure provides an example of how to upgrade your SEM components from an existing version to the latest version in the upgrade path.

1. Ensure that you have a snapshot of your existing deployment.
2. In the [supported upgrade paths](#) table, locate the SEM version that is currently running in your deployment.
3. Run the SEM Upgrade ISO for the first SEM version listed in the upgrade path.
4. When the installation is completed, ensure that:
 - You can connect to the SEM Console.
 - Your SEM deployment is functioning properly.
 - All SEM Windows agents are upgraded, connected, and sending logs and events to the SEM Manager.
5. Take a snapshot of your upgraded deployment.
6. Repeat step 3 through step 5 for each remaining SEM ISO listed in the upgrade path.

Supported upgrade paths

The following table provides the upgrade paths from a specific SEM version to the latest version.

SEM version	Upgrade path
2023.4.1	<p>Upgrade path:</p> <p>Run the SEM Upgrade ISO with the latest version.</p> <p>For example, if you are upgrading to version 2024.2, run the SEM Upgrade ISO installer that includes 2024.2.</p>

SEM version	Upgrade path
2023.4	Upgrade path: Run the SEM Upgrade ISO with the latest version. For example, if you are upgrading to version 2024.2, run the SEM Upgrade ISO installer that includes 2024.2.
2023.2.1	Upgrade path: <ol style="list-style-type: none">1. Run the SEM Upgrade ISO with version 2023.4.2. Run the SEM Upgrade ISO with the latest version.
2023.2	Upgrade path: <ol style="list-style-type: none">1. Run the SEM Upgrade ISO with version 2023.2.12. Run the SEM Upgrade ISO with version 2023.4.3. Run the SEM Upgrade ISO with the latest version.
2022.4.1	Upgrade path: <ol style="list-style-type: none">1. Run the SEM Upgrade ISO with version 2023.2.2. Run the SEM Upgrade ISO with version 2023.2.1.3. Run the SEM Upgrade ISO with version 2023.4.4. Run the SEM Upgrade ISO with the latest version.


End of Engineering versions

SEM version	Upgrade path
2022.4	Upgrade path: <ol style="list-style-type: none">1. Run the SEM Upgrade ISO with version 2022.4.1.2. Run the SEM Upgrade ISO with version 2023.2.3. Run the SEM Upgrade ISO with version 2023.2.14. Run the SEM Upgrade ISO with version 2023.4.5. Run the SEM Upgrade ISO with the latest version.

SEM version	Upgrade path
2022.2.2	Upgrade path:
2022.2.1	1. Run the SEM Upgrade ISO with version 2022.4.
2022.2	2. Run the SEM Upgrade ISO with version 2022.4.1.
	3. Run the SEM Upgrade ISO with version 2023.2.
	4. Run the SEM Upgrade ISO with version 2023.2.1.
	5. Run the SEM Upgrade ISO with version 2023.4.
	6. Run the SEM Upgrade ISO with the latest version.
2021.4	Upgrade path:
2021.2.1	1. Run the Security Event Manager - Recovery Boot CD.
2021.2	2. Run the SEM Upgrade ISO with version 2022.4.
	3. Run the SEM Upgrade ISO with version 2022.4.1.
	4. Run the SEM Upgrade ISO with version 2023.2.
	5. Run the SEM Upgrade ISO with version 2023.2.1.
	6. Run the SEM Upgrade ISO with version 2023.4.
	7. Run the SEM Upgrade ISO with the latest version.

End of Life versions

The following table provides the upgrade paths from previous LEM and SEM versions to the latest SEM version.

 Contact [SolarWinds Technical Support or Customer Service](#) for access to all End of Life versions required to upgrade your current version to the latest version.

LEM version	Upgrade path to SEM
2020.4.1	Upgrade path:
2020.4	1. Run the Security Event Manager - Recovery Boot CD.
2020.2.2	2. Run the SEM Upgrade ISO installer with version 2022.4.
	3. Run the SEM Upgrade ISO with version 2022.4.1.
	4. Run the SEM Upgrade ISO with version 2023.2.
	5. Run the SEM Upgrade ISO with version 2023.2.1.
	6. Run the SEM Upgrade ISO with version 2023.4.
	7. Run the SEM Upgrade ISO with the latest version.
2020.2.1	Upgrade path:
2020.2	1. Run the Security Event Manager - Recovery Boot CD.
2019.4	2. Run the SEM Upgrade ISO with version 2021.2.1
	3. Run the Security Event Manager - Recovery Boot CD.
	4. Run the SEM Upgrade ISO with version 2022.4.
	5. Run the SEM Upgrade ISO with version 2022.4.1.
	6. Run the SEM Upgrade ISO with version 2023.2.
	7. Run the SEM Upgrade ISO with version 2023.2.1.
	8. Run the SEM Upgrade ISO with version 2023.4.
	9. Run the SEM Upgrade ISO with the latest version.


LEM version	Upgrade path to SEM
6.7.2	Upgrade path:
6.7.1	1. Run the Security Event Manager - Recovery Boot CD.
6.7	2. Run the SEM Upgrade ISO with version 2020.2.2.
6.6	3. Run the Security Event Manager - Recovery Boot CD.
6.5	4. Run the SEM Upgrade ISO with version 2022.4.
6.4	5. Run the SEM Upgrade ISO with version 2022.4.1.
	6. Run the SEM Upgrade ISO with version 2023.2.
	7. Run the SEM Upgrade ISO with version 2023.2.1.
	8. Run the SEM Upgrade ISO with version 2023.4.
	9. Run the SEM Upgrade ISO with the latest version.
6.3.1 *	Upgrade path:
	1. Run the Security Event Manager - Recovery Boot CD.
	2. Run the SEM Upgrade ISO with version 6.4.
	3. Run the Security Event Manager - Recovery Boot CD
	4. Run the SEM Upgrade ISO with version 2020.2.2.
	5. Run the Security Event Manager - Recovery Boot CD.
	6. Run the SEM Upgrade ISO with version 2022.4.
	7. Run the SEM Upgrade ISO with version 2022.4.1.
	8. Run the SEM Upgrade ISO with version 2023.2.
	9. Run the SEM Upgrade ISO with version 2023.2.1.
	10. Run the SEM Upgrade ISO with version 2023.4.
	11. Run the SEM Upgrade ISO with the latest version.

LEM version	Upgrade path to SEM
6.3.0 *	Upgrade path:
6.2.x	<ol style="list-style-type: none">1. Run the Security Event Manager - Recovery Boot CD.2. Run the SEM Upgrade ISO with version 6.3.1.3. Run the Security Event Manager - Recovery Boot CD.4. Run the SEM Upgrade ISO with version 6.4.5. Run the Security Event Manager - Recovery Boot CD.6. Run the SEM Upgrade ISO with version 2020.2.2.7. Run the Security Event Manager - Recovery Boot CD.8. Run the SEM Upgrade ISO with version 2022.4.9. Run the SEM Upgrade ISO with version 2022.4.1.10. Run the SEM Upgrade ISO with version 2023.2.11. Run the SEM Upgrade ISO with version 2023.2.1.12. Run the SEM Upgrade ISO with version 2023.4.13. Run the SEM Upgrade ISO with the latest version.


LEM version	Upgrade path to SEM
6.1 *	Upgrade path:
6.0.1 *	<ol style="list-style-type: none">1. Run the Security Event Manager - Recovery Boot CD.2. Run the SEM Upgrade ISO with version 6.2.x.3. Run the Security Event Manager - Recovery Boot CD.4. Run the SEM Upgrade ISO with version 6.3.1.5. Run the Security Event Manager - Recovery Boot CD.6. Run the SEM Upgrade ISO with version 6.4.7. Run the Security Event Manager - Recovery Boot CD.8. Run the SEM Upgrade ISO with version 2020.2.2.9. Run the Security Event Manager - Recovery Boot CD.10. Run the SEM Upgrade ISO with version 2022.4.11. Run the SEM Upgrade ISO with version 2022.4.1.12. Run the SEM Upgrade ISO with version 2023.2.13. Run the SEM Upgrade ISO with version 2023.2.1.14. Run the SEM Upgrade ISO with version 2023.4.15. Run the SEM Upgrade ISO with the latest version.


LEM version	Upgrade path to SEM
6.0*	<p>Upgrade path:</p> <ol style="list-style-type: none"> 1. Run the Security Event Manager - Recovery Boot CD. 2. Run the SEM Upgrade ISO that includes 6.0.1. 3. Run the Security Event Manager - Recovery Boot CD. 4. Run the SEM Upgrade ISO that includes 6.2.1. 5. Run the Security Event Manager - Recovery Boot CD. 6. Run the SEM Upgrade ISO that includes 6.3.1. 7. Run the Security Event Manager - Recovery Boot CD. 8. Run the SEM Upgrade ISO that includes 6.4. 9. Run the Security Event Manager - Recovery Boot CD. 10. Run the SEM Upgrade ISO that includes 2020.2. 11. Run the SEM Upgrade ISO that includes 2022.2. 12. Run the SEM Upgrade ISO that includes 2022.4. 13. Run the SEM Upgrade ISO that includes 2022.4.1. 14. Run the SEM Upgrade ISO with version 2023.2. 15. Run the SEM Upgrade ISO with version 2023.2.1. 16. Run the SEM Upgrade ISO with version 2023.4. 17. Run the SEM Upgrade ISO that includes the latest version.

* If SMB1 is disabled during the upgrade process, upgrade to 6.3.1 hotfix 7 to perform an ISO upgrade before moving to version 6.4.

 Server Message Block version 1 (SMB1) is no longer supported.


Best practices for SEM upgrades

 As of version SEM 6.7, L4 configuration is no longer supported.

 The upgrade overwrites the system partition and cannot be interrupted or undone. SolarWinds recommends exporting (Hyper-V) or taking a snapshot of (vSphere) your SEM virtual appliance before you perform the upgrade. You can delete the snapshot when the upgrade is completed.


Resize the SEM virtual appliance

You can increase the SEM virtual appliance capacity by increasing the SEM virtual appliance size in your hypervisor. This process adds up to 15 minutes to the boot-up process to adjust the file systems.

 See your hypervisor documentation for information about increasing the appliance size.

During the boot-up process, do not turn off or reboot the appliance until the startup is completed. Subsequent bootups and reboots do not require an additional amount of time.

To retain your log data for an extended amount of time, you may need to increase the SEM virtual appliance size. You can increase your SEM virtual appliance capacity by increasing the hard disk size in your VMWare vSphere or Microsoft Hyper-V client.

 Always shut down the SEM virtual appliance before you reconfigure the vSphere or Hyper-V client disk.

When you increase the size of your virtual appliance, use the following guidelines:

- You can exceed the 2 TB limit with a fresh SEM deployment.
- After you increase the virtual disk size, you cannot decrease its size using the same methods.
- If you have VM snapshots, you cannot increase the size of your virtual appliance.

Additional considerations for VMware vSphere


If you are running VMware vSphere and do not have snapshots, you can edit the VM settings and change the disk size. During startup, the virtual appliance recognizes the change in disk size and partitions and adjusts the file systems appropriately. If snapshots are available, the disk size field is disabled.

If you need to increase the size of your virtual appliance, delete all VM snapshots or increase the existing VM by cloning it onto a larger disk. See your vSphere documentation for more information about performing these tasks.

Upgrade the SEM components

Upgrade your SEM and components in the following order. Click each link for upgrade instructions.

1. [Virtual appliance](#)
2. [Connectors](#)
3. [Consoles](#)
4. [Agents](#)

 When you perform a SEM upgrade, always reboot the SEM appliances.

Debian upgrade options

Upgrade 6.4 and later versions using the network SMB share.


Custom changes made on any SEM appliance (by root) will not be preserved after the upgrade. Specifically, any unexpected configuration formats created outside of the CMC. This includes:

- Iptables custom rules
- Modified scripts
- Added scripts
- Modified chron scheduler

Upgrade the virtual appliance

You can upgrade your SEM appliance to the latest SEM version. During this procedure, the upgrade script disconnects the SEM virtual appliance from all SEM agents and consoles.

1. Download the virtual appliance ISO package from the SolarWinds Customer Portal.

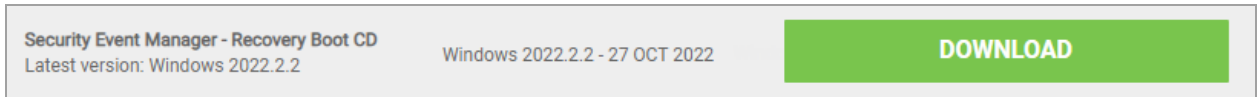
 The download requires about 400 MB of disk space.

- a. Determine the upgrade path from your current release to the latest release. Record all installers that must be downloaded for your upgrade path.

See [Determine the upgrade path](#) for instructions.

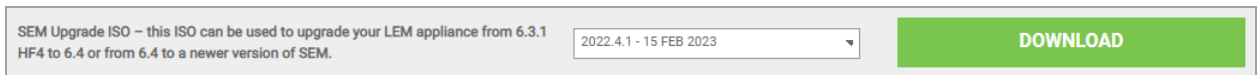
- b. Log in to the [SolarWinds Customer Portal](#) using your SolarWinds ID (SWI).
- c. Click Downloads > Download Product.

- d. Click the Products drop-down menu and select:
Security Event Manager (SEM), formerly Log & Event Manager (LEM)
- e. Click the Licenses drop-down menu and select your license tier.
- f. If you are upgrading from SEM 2021.4 or earlier, download the Security Event Manager - Recovery Boot CD located under All Release Downloads. Otherwise, go to the next step.




- g. Download the SEM Upgrade ISO installer for your upgrade version.

For example, if you need to upgrade to version 2022.4.1 in the upgrade path, click the drop-down menu, select 2022.4.1, and download this installer.



- h. Using your list from step 1a, repeat step g for each additional installer required in the upgrade path, including the installer for the latest release.
- i. Copy the upgrade files to a shared network folder.

 This step applies to any SMB share functionality in CMC.

2. Connect to the SEM virtual appliance using the virtual console (vSphere or Hyper-V Manager) or an SSH client (such as PuTTY).


If you are using an SSH client, use port 22 or 32022, and then log in with your CMC user credentials.

3. Access the CMC prompt.

In vSphere, arrow down to Advanced Configuration, and then press Enter.

In PuTTY, log in using your CMC credentials.

4. Locate the first installer in your upgrade path.
5. At the `cmc>` prompt, enter `upgrade`.
6. Follow the on-screen instructions to run the installer on the SEM appliance.

 During the upgrade, SEM may require a reboot.

7. Repeat step 4 through 5 to install all remaining installers in your upgrade path.

Troubleshoot errors during the upgrade

If you encounter errors during the upgrade, review the error message information below before you contact [Customer Support](#).

Error Message	Resolution
An error occurred during the upgrade.	Attempt to upgrade again. If the second attempt fails, pull the debugging information and open a Customer Support ticket .
You must upgrade to 2020.2 before upgrading to 2024.2.1.	See Determine the upgrade path for the appropriate upgrade procedure.

Prepare and share information with Customer Support


Use the `debug` command on your SEM virtual appliance to pull log files from the appliance to share with Customer Support. These files contain debugging information used by Customer Support to troubleshoot your issue.

Pull debugging information from your SEM virtual appliance

1. Connect to your SEM virtual appliance using the vSphere console view or an SSH client (such as PuTTY).

If you are using an SSH client, log in to your SEM virtual appliance using your CMC credentials.

2. At the `cmc>` prompt, enter `manager`, and then press Enter.
3. At the `cmc::manager` prompt, enter `debug`, and then press Enter.
4. Follow the prompts on your screen to generate the files.
5. Verify that the script generated the `.tgz` file.
6. Use Samba to share the `.tgz` file with Customer Support.


 This file does not contain alert data or other data from your SEM database.

7. Enter `exit` to return to the `cmc>` prompt.
8. Enter `exit` to log out of your SEM virtual appliance.

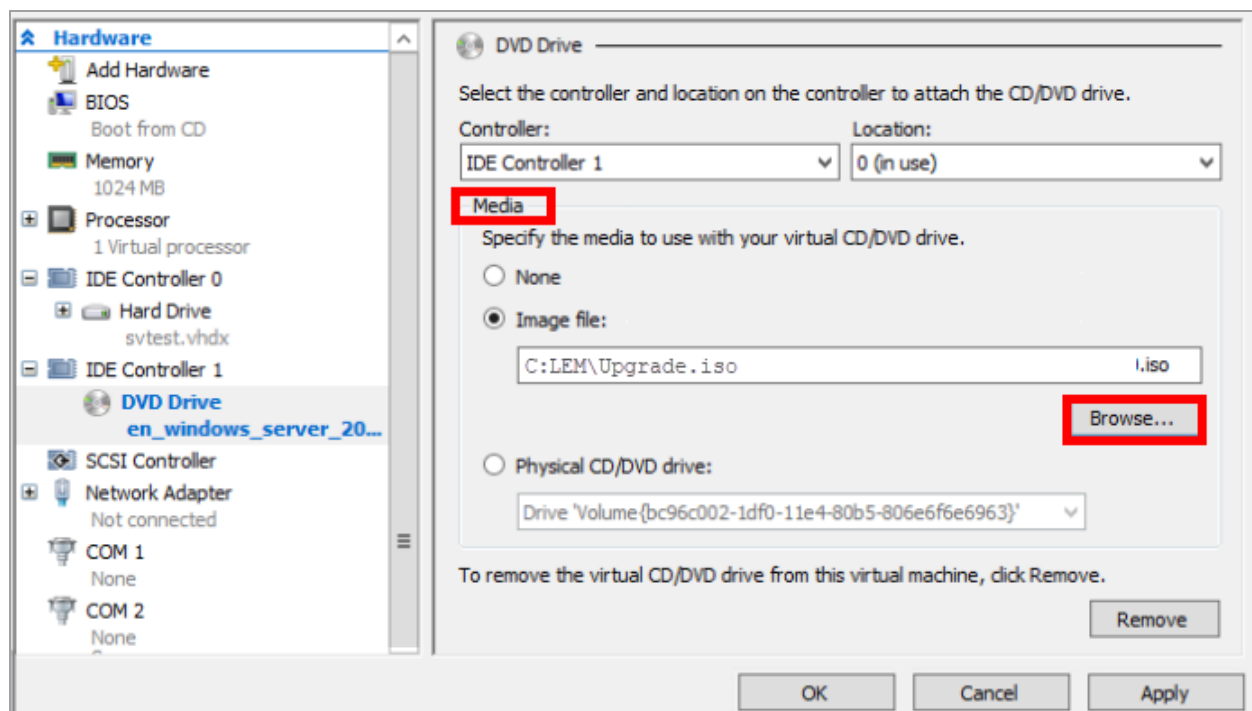
Mount the ISO image file

Download the SEM Upgrade ISO image file from the SolarWinds Customer Portal. When you are finished, mount the image on Microsoft Hyper-V or VMware vSphere.

Mount the image on Microsoft Hyper-V

 See the Microsoft Hyper-V documentation for additional information.

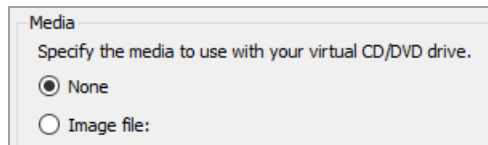
1. Right-click the virtual machine and select Settings.
2. In the left pane, select the DVD drive.



3. In the Media pane, click Browse, and then select the ISO image.
4. Click Apply, and then OK.

Unmount the image

1. Right-click the virtual machine and select Settings.
2. In the left pane, select the DVD drive.
3. Under Media select None.



4. Click Apply.

When you reopen Settings and DVD drive, the image file no longer displays in the window.

Mount the image on VMware vSphere

 See the VMware vSphere documentation for additional information.

1. Start the VMware vSphere Client.
2. Log in with administrator privileges.
3. In the left navigation pane, right-click the VM and select Edit Settings.
4. In the Virtual Machine Properties window, click CD/DVD Drive 1 and select your ISO file.
5. In the Device Type section, select Client Device, and then click OK to save the changes.
6. Start the VM before you mount the ISO.

Right-click the VM and select Power > Power On.

7. In the top menu, click the CD-ROM icon, and then select CD/DVD Drive 1 > Connect to ISO image on the local disk.

Upgrade to SEM 6.4 or later using an ISO

Beginning in SEM 6.3.1 Hotfix 5, you can upgrade to SEM 6.4 or later to the latest version using the SEM Upgrade ISO installer and the Security Event Manager - Recovery Boot CD located on the [SolarWinds Customer Portal](#).

The **Security Event Manager - Recovery Boot CD** installer provides the necessary files to support older versions in the upgrade path. If you are running an End of Life or End of Engineering version, run the CD where indicated between each version in the upgrade path.

The **SEM Upgrade ISO** installer upgrades your deployment with a version you select and download in the Customer Portal. Based on the upgrade path, you will download several versions of the SEM Upgrade ISO.

1. Back up your SEM deployment.
2. Determine the upgrade path from SEM 6.4 to the latest release.
 - a. Go to [Determine the upgrade path](#).
 - b. Scroll down to End of Life versions.
 - c. In the LEM version column, locate version 6.4.
 - d. Under Upgrade path, record the SEM Upgrade ISO installers required to upgrade to the latest version.

For example:

LEM version	Upgrade path to SEM
6.7.2	▼ Upgrade path:
6.7.1	1. Run the Security Event Manager - Recovery Boot CD.
6.7	2. Run the SEM Upgrade ISO with version 2020.2.2.
6.6	3. Run the Security Event Manager - Recovery Boot CD.
6.5	4. Run the SEM Upgrade ISO with version 2022.4.
6.4	5. Run the SEM Upgrade ISO with version 2022.4.1.
	6. Run the SEM Upgrade ISO with the latest version.

3. Download the Security Event Manager - Recovery Boot CD from the SolarWinds Customer Portal.
 - a. Log in to the [SolarWinds Customer Portal](#) using your SolarWinds ID (SWI).
 - b. Click Downloads > Download Product.
 - c. Click the Products drop-down menu and select:

Security Event Manager (SEM), formerly Log & Event Manager (LEM).
 - d. Click the Licenses drop-down menu and select your license tier.
 - e. Scroll down to All Release Downloads and locate the Security Event Manager - Recovery Boot CD.

Security Event Manager - Recovery Boot CD Latest version: Windows 2022.2.2	Windows 2022.2.2 - 27 OCT 2022
--	--------------------------------

- f. Click Download.

- g. Click the SEM Upgrade ISO drop-down menu, select the targeted release version, and then click Download.
- h. When prompted, click Finish Download.

The installer is downloaded to your system.

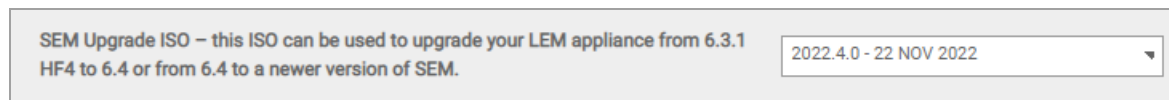
`SolarWinds-SEM-<version>-Recovery-CD.iso`

where `<version>` is the version listed for the installer.

For example:

`SolarWinds-SEM-2022.2-Recovery-CD.iso`

4. Download the SEM Upgrade ISO installers from the SolarWinds Customer Portal.
 - a. Locate the list of installers you recorded in step 1.
 - b. Return to the Product Downloads page.
 - c. Scroll down to Upgrade Downloads and locate the SEM Upgrade ISO installer.



- d. Click the product version drop-down menu and select a version that matches the lowest version in your list. For example, version 2022.4.0.
 - e. Click Download to download the installer.
 - f. When prompted, click Finish Download.

The installer is downloaded to your system.


`SolarWinds-SEM-<version>-Upgrade.iso`

For example:


`SolarWinds-SEM-2022-4-Upgrade.iso`

- g. Repeat step b through step f for each additional installer in your list.
5. Mount the ISO images you downloaded in step 2 and step 3 on your hypervisor.

See [Mount the ISO image](#) for instructions.

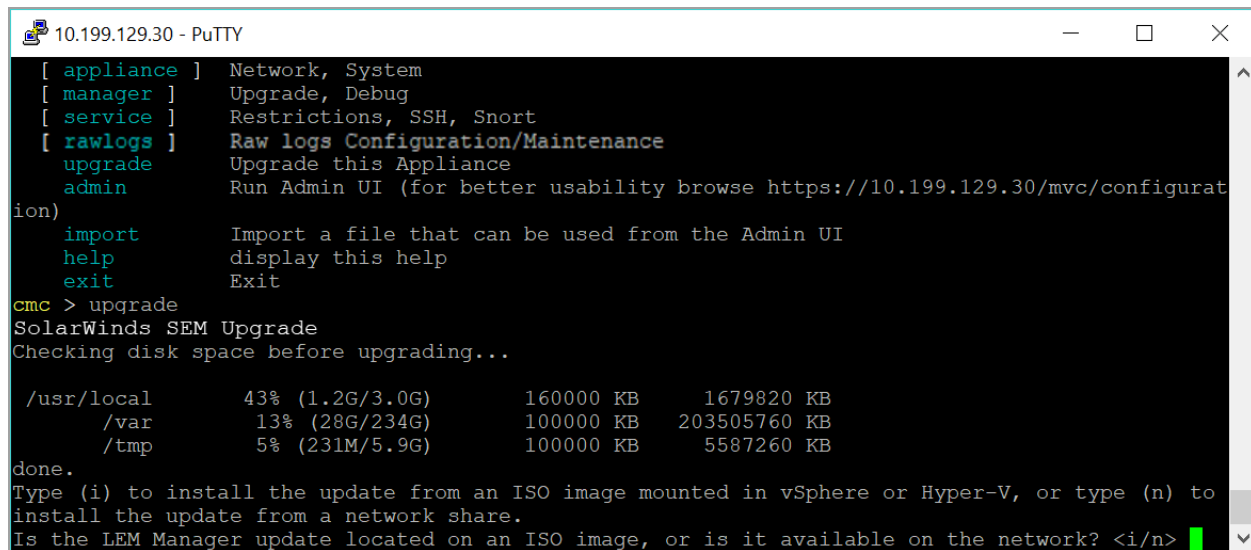
 During the upgrade procedure, the upgrade script disconnects the SEM virtual appliance from all SEM agents and consoles.

6. Connect to the SEM virtual appliance using the vSphere or Hyper-V Manager virtual console or an SSH client (such as PuTTY).

 Use port 22 when using an SSH client.

7. Log in with your CMC user credentials.
8. Access the CMC prompt.
9. In vSphere, arrow down to Advanced Configuration, and then press Enter.
10. In PuTTY, log in using your CMC credentials.
11. At the CMC > prompt, enter:

upgrade




```

10.199.129.30 - PuTTY
[ appliance ] Network, System
[ manager ] Upgrade, Debug
[ service ] Restrictions, SSH, Snort
[ rawlogs ] Raw logs Configuration/Maintenance
[ upgrade ] Upgrade this Appliance
[ admin ] Run Admin UI (for better usability browse https://10.199.129.30/mvc/configurat
ion)
[ import ] Import a file that can be used from the Admin UI
[ help ] display this help
[ exit ] Exit
cmc > upgrade
SolarWinds SEM Upgrade
Checking disk space before upgrading...

/usr/local      43% (1.2G/3.0G)      160000 KB      1679820 KB
/var            13% (28G/234G)      100000 KB      203505760 KB
/tmp            5% (231M/5.9G)      100000 KB      5587260 KB
done.
Type (i) to install the update from an ISO image mounted in vSphere or Hyper-V, or type (n) to
install the update from a network share.
Is the LEM Manager update located on an ISO image, or is it available on the network? <i/n>

```

12. Upload the ISO images **in the listed order** for your upgrade path.

 During the procedure, you will upload the Security Event Manager - Recovery Boot CD installer twice. This procedure provides the needed files to support the next ISO installer in your list.

- a. Enter **i** for ISO, and then follow the prompts to install the first ISO in your list.
 - b. Reboot the SEM appliance.
 - c. Repeat step 5 through step 11b for each additional ISO file in the list.
13. Unmount the images from your hypervisor.

See [Mount the ISO image](#) for instructions.


Upgrade to SEM 6.4 or later across a network share

Beginning in SEM 6.3.1 Hotfix 5, you can upgrade to SEM 6.4 or later to the latest version using the SEM Upgrade ISO installer and the Security Event Manager - Recovery Boot CD located on the [SolarWinds Customer Portal](#).


The **Security Event Manager - Recovery Boot CD** installer provides the necessary files to support older versions in the upgrade path. If you are running an End of Life or End of Engineering version, run the CD where indicated between each version in the upgrade path.

The **SEM Upgrade ISO** installer upgrades your deployment with a version you select and download in the Customer Portal. Based on the upgrade path, you will download several versions of the SEM Upgrade ISO.


1. Back up your SEM deployment.
2. Prepare the upgrade media.
 - a. Complete step 1 through step 4 in [Upgrade to SEM 6.4 or later using an ISO](#).
 - b. Place the ISO installers on the network share drive.

 The upgrade network path should look similar to:
`\\<server- IP>\<SEM>`

3. Connect to the SEM virtual appliance using the vSphere or Hyper-V Manager virtual console or an SSH client (such as PuTTY).

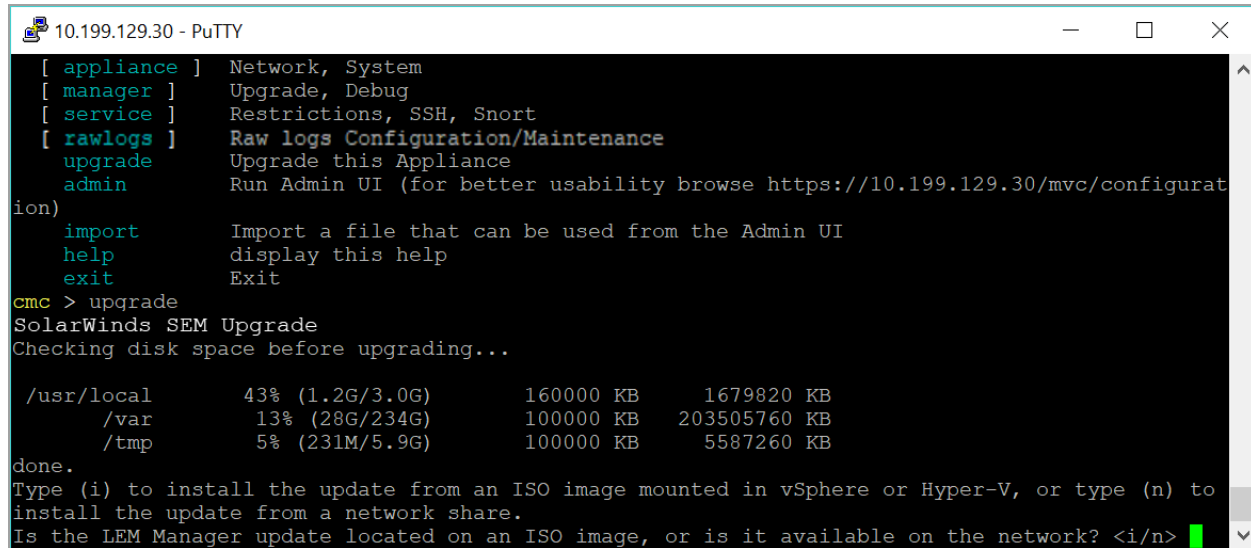
 Use port 22 when using an SSH client.

4. Log in with your CMC user credentials.

 During the upgrade process, the upgrade script disconnects the SEM virtual appliance from all SEM agents and consoles.

5. Access the CMC prompt.
6. In vSphere, arrow down to Advanced Configuration, and then press Enter.
7. In PuTTY, log in using your CMC credentials.

8. At the CMC > prompt, enter: `upgrade`



```


10.199.129.30 - PuTTY
[ appliance ] Network, System
[ manager ] Upgrade, Debug
[ service ] Restrictions, SSH, Snort
[ rawlogs ] Raw logs Configuration/Maintenance
[ upgrade ] Upgrade this Appliance
[ admin ] Run Admin UI (for better usability browse https://10.199.129.30/mvc/configuration)
import Import a file that can be used from the Admin UI
help display this help
exit Exit
cmc > upgrade
SolarWinds SEM Upgrade
Checking disk space before upgrading...

/usr/local      43% (1.2G/3.0G)      160000 KB      1679820 KB
/var            13% (28G/234G)      100000 KB      203505760 KB
/tmp            5% (231M/5.9G)      100000 KB      5587260 KB

done.
Type (i) to install the update from an ISO image mounted in vSphere or Hyper-V, or type (n) to
install the update from a network share.
Is the LEM Manager update located on an ISO image, or is it available on the network? <i/n>


```

9. Upload the ISO images **in the listed order** for your upgrade path.

 During the procedure, you will upload the Security Event Manager - Recovery Boot CD installer twice. This procedure provides the needed files to support the next ISO installer in your upgrade path.

- a. Enter `n` for network, and then follow the prompts to complete the installation.
 - b. Reboot the SEM appliance.
 - c. Repeat step 3 through step 8b for each additional ISO file in the upgrade path.
10. Unmount the images from your hypervisor.
- See [Mount the ISO image](#) for instructions.

Upgrade the connectors

 For versions prior to 6.2.0, update your connectors using the CMC command interface.


Upgrade the connectors using the SEM Console

1. Log in to SEM as an administrator.
2. In the SEM Console toolbar, click Settings.



3. In the left column, click Updates.
4. Under Connector Updates, click Update now.

A confirmation message displays on the screen, indicating the update status.

 To enable automatic updates, move the Allow automatic updates toggle to the right.

Upgrade the connectors using the CMC interface

1. Download the latest connectors from the SolarWinds Customer Portal.
 - a. Log in to the [SolarWinds Customer Portal](#) using your SolarWinds ID (SWI).
 - b. Click Downloads > Download Product.
 - c. Click the Products drop-down menu and select Security Event Manager (SEM), formerly Log & Event Manager (LEM).
 - d. Click the Licenses drop-down menu and select your license tier.
 - e. Scroll down to Upgrade Downloads.
 - f. Locate Latest Connector Update Package and click Download.
 - g. If prompted, click Finish Download.

The package ZIP file is downloaded to your system.

For example:

`SolarWinds-SEM-<version>-Upgrade.zip`

where `<version>` is the SEM release version.

For example:

`SolarWinds-SEM-2022.4-Upgrade.zip`

2. Prepare the update package.
 - a. Unzip the package file.

 The directory structure uses approximately 390 MB of disk space.

- b. Open the package folder.
- c. Copy the folder to the root of a network share.

For example:

```
\\<server-IP>\<share-name>
```

The connector locates the SEM directory under the root of the share.

3. Connect to the SEM virtual appliance using a virtual console or SSH client.
4. Access the `cmc>` prompt.

If you are using a virtual console, scroll down to Advanced Configuration, and then press Enter.

If you are using an SSH Client, log in using your CMC credentials.

5. Update the connectors.



```

  _____
 /  _  _  _  \
/  _ \| | | | \
)_  _ \| | | |
|_|_|_|_|_|_|_|

                                SolarWinds
                                Security Event Manager

Last login: Wed Oct 27 12:44:28 2021 from
////////////////////////////////////
///      SolarWinds Security Event Manager      ///
///                               management console                               ///
////////////////////////////////////

Detected VMware Virtual Platform
Product Support Key:
Available commands:
[ appliance ] Network, System
[ manager   ] Upgrade, Debug
[ service   ] Restrictions, SSH
[ rawlogs   ] Raw logs Configuration/Maintenance
upgrade      Upgrade this Appliance
help         display this help
exit         Exit
cmc >

```

 Press Enter after entering each command.

- a. At the `cmc>` prompt, enter `manager`.
- b. At the `cmc::manager` prompt, enter `sensortoolupgrade`.
- c. Press Enter to begin the upgrade process.
- d. Enter your Windows destination share.

For example: `\\server\share: \\share\folder\`

- e. When prompted (see below), enter your user name and password.
 - Please enter the username, including any domain information (e.g. DOMAIN\user):
 - Please enter the password:
6. Verify that the configured connectors restart after the update by monitoring the SEM console and searching for `InternalToolOnline` events in the default SolarWinds events filter.
7. When the update is completed, enter `exit` twice to exit the CMC interface.

Upgrade the web console

Upgrading the SEM appliance automatically updates the SEM web console. During the upgrade, you may be reconnected automatically. To ensure you are running the latest web console version, you can:

- Refresh the console in your browser
- Close the console, reopen your browser, and reconnect

Upgrade the agents

To take advantage of new enhancements such as Java Runtime Environment (JRE) and infrastructure updates, be sure to upgrade the SEM agents.

If you selected the Enable Global Automatic Updates check box when you [adjusted your Global Automatic Update setting](#), your SEM agents will update automatically. If you did not enable global automatic updates, you can manually upgrade the SEM agents by accessing the installer through the SEM Console or using an installer downloaded directly from the [SolarWinds Customer Portal](#).

After you upgrade the SEM agents, [adjust the Agent Updates](#) setting.

Upgrade SEM agents for Windows using the SEM Console


If your console is connected to the Internet, you can update your SEM agents through the SEM Console.

1. Log in to SEM as an administrator.
2. On the SEM Console toolbar, click Configure > Nodes.
3. On the Nodes toolbar, click Add agent node.
4. Select the appropriate installation type.

Select Remote Installation to push SEM agents to Microsoft Windows hosts across your network.

Select Local Installation to log in to the device and install the SEM agent.

5. Copy the `setup.exe` file to the local hard drive on the computer.

 The security settings in some Windows operating systems require the installer to be on the local hard drive prior to the launch.


6. Right-click the installer, select Run as Administrator, and then complete the installation wizard.

Upgrade SEM agents for Windows using an installer

If your console is not connected to the Internet, you can update your SEM agents by downloading the agent installer from another computer with an Internet connection.

Install your new SEM agents in the same folder as your existing SEM agents. This process allows the installer to update the SEM agent software while maintaining all other configuration settings.

1. Download the agent installer from the Additional Components page on the [SolarWinds Customer Portal](#).
2. Extract the ZIP file contents to your desktop or another location.
3. Copy the `SolarWinds-SEM-2022.2-Agent-WindowsInstaller.exe` file to the local hard drive on the computer.

 The security settings in some Windows operating systems require the installer to be on the local hard drive prior to the launch.

4. Right-click `setup.exe`, select Run as Administrator, and then complete the installation wizard.

Adjust the Agent Updates setting


Before you upgrade SEM, ensure that the Agent Updates setting for your SEM agents is configured correctly. When enabled, agent upgrades occur automatically when available. Disable this option if change management or other testing is required for agent upgrades.

On the SEM Console Settings page, you can enable automatic updates for SEM agents and set the number of concurrent updates.

1. Log in to SEM as an administrator.
2. On the SEM Console toolbar, click the Settings icon.



3. On the Settings page, click Updates in the left column.
4. Under Agent Updates, click the toggle button to enable automatic agent updates.
5. Set the maximum number of concurrent updates, and then click Save.


 This setting determines the number of agents that can be updated at the same time.

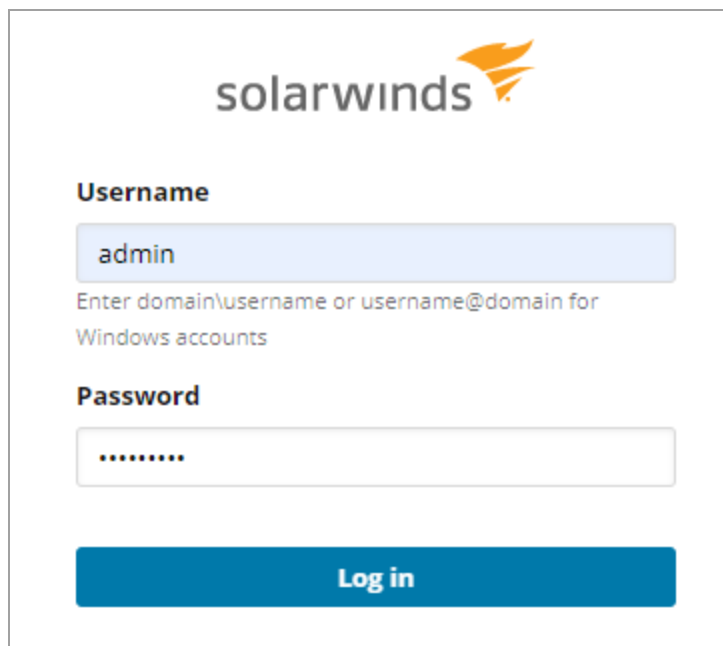
Log in to SEM

Log in to the [SEM Console](#) using the URL provided to you or the [SEM CMC command line interface](#) to perform the required administrative tasks to work with SEM.

Log in to the SEM Console

1. Locate the SEM URL provided to you.
2. Open a [supported web browser](#) window.
3. In the Address field, enter the URL to connect to the SEM console.
4. Enter your user name and password, and then click Log in.

 If SSO is enabled, you can log in by clicking Log in with SSO and using your Windows credentials.



The screenshot shows the SolarWinds login page. At the top is the SolarWinds logo. Below it, the 'Username' field contains the text 'admin'. A note below the username field says 'Enter domain\username or username@domain for Windows accounts'. The 'Password' field is masked with dots. At the bottom is a blue 'Log in' button.

Log in to the SEM CMC command line interface

Use the CMC command-line interface (CLI) to perform administrative tasks such as:

- Rebooting or shutting down the SEM VM
- Upgrading the SEM Manager software
- Applying connector updates
- Deploying new connector infrastructure to SEM Managers and Agents

There are two ways to log in to the CMC CLI:


- Connect using the console provided with your hypervisor
- Connect using a secure shell (SSH) client such as PuTTY

CMC Access Restrictions

The following access restrictions apply to the CMC command-line interface:

- You do not need an account with root access to administer SEM from the CMC command line.
- You need to enter the CMC user name and password to log in to the CMC command line using SSH. The user name is `cmc` and the default CMC password is `password`. See [Change the SEM CMC password](#) to change it.
- You need to enter the CMC username and password to login via the hypervisor console in Hyper V and VMWare.
- SSH access to the CMC interface can be restricted by IP address or host name. If enabled, this security feature blacklists everyone from logging in to the CMC interface except those users who connect from an explicitly allowed IP address or host name. See [Restrict SSH access to the CMC interface](#) for details.

Log in to the CMC command-line interface using the hypervisor virtual console

 See your hypervisor documentation for information about using the virtual console.

1. Open your hypervisor and connect to the SEM VM:

For VMware vSphere:

- a. Click the Console tab.
- b. Select Advanced Configuration on the main console screen, and press Enter to access the command prompt.

For Hyper-V:


- a. Click Action > Connect, and then click the Console tab.
- b. Use the arrow keys to navigate to Advanced Configuration, and press Enter.

2. Enter the CMC user name and password.

The CMC menu appears with a `cmc>` prompt.

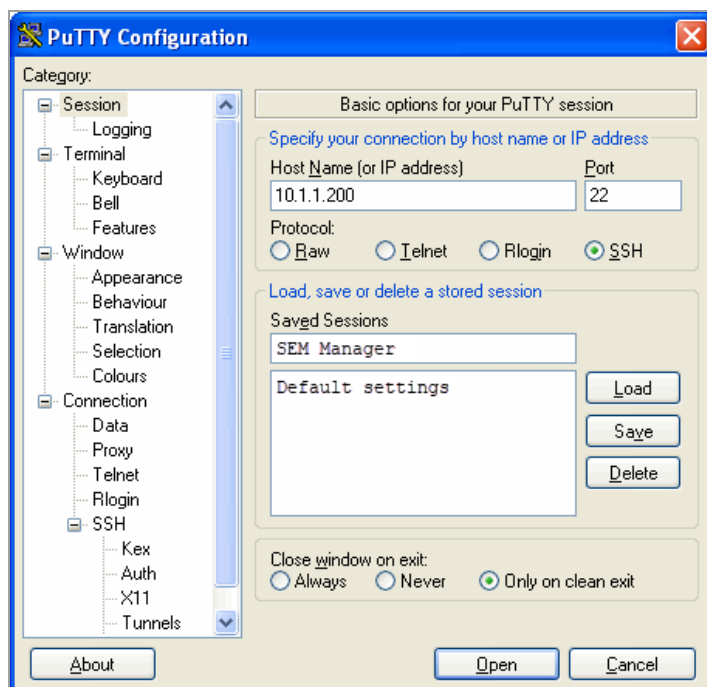
See [CMC main menu](#) for a list of top-level CMC commands.

Log in to the CMC command-line interface using SSH

 See [CMC Access Restrictions](#) for information about credentials and SSH access restrictions.

You can connect to SEM using a secure shell (SSH) client (such as PuTTY). The following steps show how to configure PuTTY to open the CMC command line, but these settings will work in any SSH client.

1. Open PuTTY and verify that Session is selected in the Category section.



Get help after you install SEM

After you install SEM, two resources are available to help you get started.

Read the [SEM Getting Started Guide](#) first to learn how to use the product.

Next, see the [SEM Administrator Guide](#) to learn more about how to configure and set up SEM for your deployment.